No. 14-3514

IN THE UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

FEDERAL TRADE COMMISSION,
Plaintiff-Appellee,

v.

WYNDHAM HOTELS & RESORTS, LLC, *et al*.,
Defendants-Appellant.

On Interlocutory Appeal From An Order Of The United States District Court
For the District Of New Jersey, Case No. 2:13-cv-01887-ES-JAD

BRIEF FOR THE FEDERAL TRADE COMMISSION

JONATHAN E. NUECHTERLEIN
General Counsel

DAVID C. SHONKA
Principal Deputy General Counsel

JOEL MARCUS
DAVID SIERADZKI
Attorneys

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Of Counsel:

KEVIN H. MORIARTY
JAMES A. TRILLING
KATHERINE E. MCCARRON
Attorneys
Bureau of Consumer Protection

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES **PAGE**

FTC CONSENT DECREES

STATUTES

RULES AND REGULATIONS

LEGISLATIVE HISTORY

MISCELLANEOUS

QUESTIONS PRESENTED

Section 5 of the Federal Trade Commission Act makes unlawful all "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). In the complaint at issue here, the Federal Trade Commission has alleged that Wyndham violated that provision by failing to take reasonable measures to protect credit card numbers that its customers entrusted to it and that it stored on its computer networks. The computer system was hacked, and the numbers were stolen and used to make fraudulent purchases. The questions presented are:

1) Whether a company's unreasonable failure to protect the security of consumer data entrusted to it can constitute an "unfair … act or practice";

2) Whether Wyndham had constitutionally sufficient notice that it needed to take reasonable steps to protect the consumer data entrusted to it; and

3) Whether the complaint sufficiently alleged that the data breaches caused consumers substantial injury that they could not have reasonably avoided.

RELATED CASES AND PROCEEDINGS

This case was before the Court previously on Wyndham's petition for leave to appeal (No. 14-8091). There are no other directly related cases or proceedings.

STANDARD OF REVIEW

The Court reviews *de novo* a district court's ruling on a motion to dismiss. The FTC's interpretation of the FTC Act, however, is entitled to deference under

Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837, 842 (1984).

STATEMENT OF THE CASE

Virtually all modern commerce involves the collection and storage of consumers' personal data, such as credit card numbers, passwords, and social security numbers. That personal information is an appealing target for hackers, who can use it to steal identities, make fraudulent purchases, and cause other harm to consumers. Yet a consumer who gives personal information to a merchant is powerless to protect that information once it is in the merchant's hands. Consumers must depend on the merchant to take reasonable measures to keep their personal data secure. Implementing such measures is thus fundamental to modern consumer protection.

Here, Wyndham ignored multiple warning signs that its network had been compromised, and it failed to address repeated and obvious security lapses that left its computer networks vulnerable to intruders. As a result, hackers infiltrated Wyndham's computer network and stole customer credit card information, which was used to make millions of dollars in fraudulent charges on the accounts of Wyndham's customers. The FTC sued Wyndham for failing to take reasonable steps to protect its customers' data. That failure, the FTC's complaint charged in

relevant part, violated the prohibition on "unfair … acts or practices" in Section 5 of the FTC Act, 15 U.S.C. § 45.

Wyndham moved under Fed. R. Civ. P. 12(b)(6) to dismiss the complaint on various grounds. The district court denied that motion in a detailed opinion, and Wyndham has now taken this interlocutory appeal. Because this appeal arises from the denial of a Rule 12(b)(6) motion, this Court is "required to accept as true all allegations in the complaint and all reasonable inferences that can be drawn therefrom, and view them in the light most favorable to" the FTC. *Evancho v. Fisher*, 423 F.3d 347, 350 (3d Cir. 2005). The discussion below likewise assumes that the complaint's allegations have been proven.

1. The Statutory Scheme

Section 5(a) of the FTC Act broadly prohibits all "unfair or deceptive acts or practices in or affecting commerce" and "empower[s] and direct[s]" the FTC to prevent such acts, except in certain defined market contexts. 15 U.S.C. § 45(a)(1), (2). This appeal involves a claim under the "unfair practices" provision of Section 5.[1] Because the modern economy gives rise to a limitless variety of unfair practices, courts have long read the broad language of this provision as leaving it to the FTC in the first instance "to determine what practices [are] unfair." *FTC v.*

[1] The FTC also brought a distinct claim against Wyndham under the "deceptive practices" provision. Wyndham does not appeal the district court's denial of its motion to dismiss that claim.

Sperry & Hutchinson Co., 405 U.S. 233, 240 (1972). By "intentionally le[aving] development of the term 'unfair' to the Commission," *Atl. Ref. Co. v. FTC*, 381 U.S. 357, 367 (1965), Congress gave the FTC broad discretion to "'prevent such acts or practices which injuriously affect the general public.'" *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 967 (D.C. Cir. 1985) (quoting H.R. Rep. No. 1613, 75th Cong., 1st Sess. 3 (1937)).[2]

As *Sperry* confirms, Congress originally placed no greater constraint on the FTC's discretion to determine whether business practices are "unfair" than it placed on the discretion of other agencies to determine, for example, whether common carrier practices are "just and reasonable" (*e.g.*, 47 U.S.C. § 201(b)). *See* Argument § I, *infra*. In 1980, responding to "criticism of the vagueness and breadth of the unfairness doctrine," *American Financial*, 767 F.2d at 969, the FTC issued a policy statement limiting the scope of unfair practices to business conduct that causes consumers substantial injury that they cannot reasonably avoid and that

[2] As initially enacted in 1914, Section 5 of the FTC Act prohibited only "unfair methods of competition." 38 Stat. 719. In 1938, Congress broadened Section 5 to also cover "unfair or deceptive acts or practices in commerce," 52 Stat. 111. The 1938 amendment is now the main source of the FTC's consumer protection authority (as distinct from its antitrust authority). Congress's intent "was affirmatively to grant the Commission authority to protect consumers as well as competitors." *American Financial*, 767 F.2d at 966. The term "unfair" thus means the same in the 1938 amendments as in the original 1914 enactment. *See Sperry*, 405 U.S. at 244.

has no countervailing benefit. *Policy Statement on Unfairness* (Dec. 17, 1980) (appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984)).

In 1994, Congress codified the *Policy Statement* in Section 5(n) of the FTC Act. *See* H.R. Rep. 103-617 at 12 (1994). Like the *Policy Statement*, Section 5(n) specifies that an act or practice may be deemed unfair only if it "[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 to competition." 15 U.S.C. § 45(n). That three-part cost-benefit test "is the most precise definition of unfairness articulated by either the Commission or Congress." *American Financial*, 767 F.2d at 972.

2. The FTC's Data-Security Program

The FTC has addressed online threats to consumers "for almost as long as there has been an online marketplace."[3] To that end, the agency engages in a variety of educational and enforcement activities, including actions directed at protecting consumer data.

In 2007, for example, the FTC published a guidance manual for businesses cataloguing reasonable data-security practices. *See Protecting Personal Information: A Guide for Business* (2007) ("Business Guide") (copy attached).

---

[3] FTC Report to Congress, *Privacy Online*, i (June 1998), http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

The Business Guide advised companies to "[i]dentify the computers or servers where sensitive personal information is stored," and to "[i]dentify all connections to the computers where you store sensitive information." *Id*. at 9. It recommended "encrypting sensitive information that is stored on your computer network," *id*. at 10, and warned that "[w]hen installing new software, immediately change vendor supplied default passwords to a more secure strong password," *id.* at 13. Companies also should "implement policies for installing vendor-approved patches to correct [security] problems." *Id*. at 10.

The Business Guide further explained that computer networks should "[u]se a firewall to protect [a] computer from hacker attacks while it is connected to the Internet." *Id.* at 14. Specifically, if "some computers on your network store sensitive information while others do not, consider using additional firewalls to protect the computers with sensitive information." *Id*. Companies should also "consider using an intrusion detection system" to alert them to security breaches, *id*. at 15, and should "[k]eep an eye out for activity from new users, multiple log-in attempts from unknown users or computers," *id*. at 16.

The Business Guide reflected the Commission's enforcement actions against individual companies, which spelled out for the business community the types of data-security deficiencies that could trigger Section 5 liability. For example, the FTC charged retailer BJ's Wholesale Club with unfair practices after hackers stole

customer information from the company's computers and used it to make fraudulent purchases. According to the complaint, BJ's had acted unreasonably by failing to encrypt data, change default passwords, detect intrusions, or conduct security investigations. *See BJ's Wholesale Club*, 140 F.T.C. 465, 467 ¶7 (Sept. 20, 2005).[4] The Commission explained that, for purposes of Section 5(n), the "failure to employ reasonable and appropriate security measures to protect personal information and files caused or is likely to cause substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers." *Id*. at 468 ¶9. After the parties decided to settle, the FTC sought public comment on a proposed consent judgment via Federal Register notice, *see* 70 Fed. Reg. 36939 (June 27, 2005). After receiving and considering comments, the agency approved the judgment, announced it in the press, and placed it and other case materials on the agency's website.

Between 2005 and 2008—the period just before Wyndham's security breaches—the Commission brought similar cases against at least eight other companies. As in *BJ's*, the Commission charged that the eight companies had failed to take reasonable data security measures, including data encryption,

[4] Available at http://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter.

intrusion detection, and the use of secure passwords and firewalls.[5] An explanation of the consent order in each matter was published in the Federal Register, approved by the Commission, announced in the press, and placed (along with other case materials) on the FTC's website.

These enforcement initiatives continue. In early 2014, the FTC announced its 50th data-security settlement. *See* Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014) ("50th Settlement Statement"), www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf. As the FTC has emphasized, the FTC Act "does not require perfect security," and "the mere fact that a breach occurred does not mean that a company has violated the law." *Id.* at 1. Instead, "[t]he touchstone of the Commission's approach to data security is reasonableness." *Id*.

---

[5] *See CardSystems Solutions, Inc.*, http://www.ftc.gov/enforcement/cases-proceedings/052-3148/cardsystems-solutions-inc-solidus-networks-inc-dba-pay-touch; *Superior Mortgage Corp.*, http://www.ftc.gov/enforcement/cases-proceedings/052-3136/superior-mortgage-corp-matter; *DSW Inc.*, http://www.ftc.gov/enforcement/cases-proceedings/052-3096/dsw-incin-matter; *Nations Title Agency, Inc.*, http://www.ftc.gov/enforcement/cases-proceedings/052-3117/nations-title-agency-inc-nations-holding-company-christopher; *Guidance Software, Inc.* http://www.ftc.gov/enforcement/cases-proceedings/062-3057/guidance-software-inc-matter; *Life is good, Inc.*, http://www.ftc.gov/enforcement/cases-proceedings/072-3046/life-good-inc-life-good-retail-inc-matter; *TJX Companies*, http://www.ftc.gov/enforcement/cases-proceedings/072-3055/tjx-companies-inc-matter; *Reed Elsevier, Inc.*, http://www.ftc.gov/enforcement/cases-proceedings/052-3094/reed-elsevier-inc-seisint-inc-matter. *See* note 16, *infra* (discussing different legal theories underlying these cases).

3. Wyndham's Data-Security Lapses

As part of its hotel business, Wyndham operates a computer network that connects its own data center with the "property management system" computers that it manages at Wyndham-branded hotels. First Amended Complaint ("Cmplt.") ¶¶13-19 (JA61-63).[6] The property management systems "handle[] reservations … and … payment card transactions" and "store personal information about consumers, including names, addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes." *Id*. ¶15 (JA62). Wyndham requires each hotel to purchase the property management system and configure it to Wyndham's specifications. *Id*. ¶15 (JA62). Wyndham manages each property management system and has exclusive "administrator access" to system controls, which includes establishing password requirements. *Id*. ¶17 (JA62-63). The individual property management systems are linked to a corporate network, housed at a data center in Phoenix, Arizona. *Id*. ¶16 (JA62).

As Wyndham informed its customers on its website, it has long "recognize[d] the importance of protecting the privacy" of personal information. Cmplt. ¶21 (JA64) (quoting Wyndham's privacy policy). Since at least 2008, Wyndham has assured its customers that it "safeguard[s] … [c]ustomers'

---

[6] As used in this brief, "Wyndham" refers collectively to the four corporate entities named in the complaint. *See* Cmplt. Ex.A (JA78). Wyndham does not argue that the formal separateness of those entities is relevant to any issue on appeal. *See* Br. n.3.

personally identifiable information by using industry standard practices," including "commercially reasonable efforts to make … collection of such [i]nformation consistent with all applicable laws and regulations." *Id*. The company promised to "utilize a variety of different security measures designed to protect" customer information, such as encrypting data, as well as "commercially reasonable efforts to create and maintain 'fire walls' and other appropriate safeguards" to protect customer data. *Id*.

Although Wyndham explicitly recognized its obligation to take reasonable steps to secure its customers' personal information, it failed to do so during the period relevant here. Among other things, Wyndham left customer data unprotected by firewalls; did not encrypt credit card information; used outdated software that could not receive security updates; used widely known default passwords and easily guessed passwords instead of complex passwords; failed to keep track of the computers connected to its network; and failed to employ reasonable measures for detecting and preventing intrusions. Cmplt. ¶24 (JA65-67). As a result, hackers infiltrated Wyndham's computer network three separate times between 2008 and 2010 and stole customer data each time.

Breach No. 1 (April 2008). The first breach involved a "brute force" attack from a local hotel network connected to the Wyndham property management system at the hotel. The intruders used this connection to try usernames and

passwords repeatedly until they were able to compromise an administrator account on the Wyndham network. Cmplt. ¶26 (JA68). That was possible because Wyndham violated basic data-security norms by using default or other easily guessed passwords. *Id*. ¶24(f) (JA66-67).

Three additional security lapses then enabled the hackers to gain access to customer data on computers throughout Wyndham's network. First, the hackers' initial brute-force attack had caused numerous user accounts to be "locked out" as the hackers moved from account to account trying to guess the passwords needed for entry into the wider network. The widespread locking out of accounts is "a well-known warning sign that a computer network is being attacked." Cmplt. ¶27 (JA68-69). Wyndham knew that account lockouts were occurring. But because it had no inventory of connected computers, it could not determine and quarantine the location of the breach. *Id*.

Second, the property management server used outdated software that its developer no longer supported, and it therefore lacked three years of security updates. Cmplt. ¶29 (JA69). Wyndham knew about the vulnerability but allowed the server, which it controlled, to connect to its network anyway. *Id*. Third, Wyndham did not use firewalls to "limit access between and among the Wyndham-branded hotels' property management systems, [Wyndham's] own corporate network, and the Internet." *Id*. ¶28 (JA69). Thus, once the hackers had

the administrator account password, "they were able to gain unfettered access" to the property management servers—and the personal data stored there—in many hotels. *Id*.

On top of these lapses, yet another security flaw gave the intruders direct access to customer data. Several property management servers, controlled by Wyndham, stored consumer credit card information "in clear readable text" rather than an encrypted format. Cmplt. ¶31 (JA69-70). The intruders were thus able to steal unencrypted information for more than 500,000 credit card accounts, export it to Russia, and facilitate fraudulent charges totaling millions of dollars. *Id*. ¶32 (JA70).

Breach No. 2 (March 2009). The second breach occurred at the Phoenix data center in March 2009, just six months after Wyndham learned of the first breach. Cmplt. ¶33 (JA70-71). The hackers gained access to nearly 40 property management servers on the network. *Id*. Wyndham did not discover the new breach because it had failed to monitor its network for the presence of malicious software used in the first attack. *Id*. The second attack used the same software, but in the absence of network monitoring, Wyndham did not learn of the second attack until it began receiving complaints of unauthorized charges to customer credit cards two months later. *Id*. In the interim, the data thieves stole more than 50,000

consumers' unencrypted credit card account data, which again enabled fraudulent charges on those accounts. *Id*. ¶¶35-36 (JA71).

Breach No. 3 (late 2009). Despite the two earlier incidents, by late 2009 Wyndham had not properly implemented firewalls. Wyndham also was not able to detect the breach in real time. Cmplt. ¶37-38 (JA71-72). Those failures enabled hackers to break undetected into Wyndham's network yet a third time. As before, the breach of an administrator account allowed the infiltrators "to access multiple … servers" across the network. *Id*. ¶37 (JA71-72). About 69,000 card numbers were stolen. *Id*. ¶39 (JA72).

In total, the three breaches led to "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." Cmplt. ¶40 (JA73).

4. Proceedings Below

The FTC's complaint separately charged Wyndham with both "unfair" and "deceptive" practices. Cmplt. ¶¶44-49 (JA73-74). Wyndham moved to dismiss the complaint on three grounds pertinent to the unfair-practices claim at issue here. It argued (1) that Section 5 does not authorize the FTC to bring an unfairness claim for unreasonable data-security practices; (2) that the FTC had not provided fair

notice of the security standards required under Section 5; and (3) that the complaint did not allege facts sufficient to show harm to consumers as required by Section 5(n). Dkt. Entry 91-1 (April 26, 2013).

The district court denied the motion to dismiss in a 42-page opinion. It first declined Wyndham's "invitation to carve out a data-security exception to the FTC's unfairness authority." *Opinion* 10 (JA11). And it rejected Wyndham's claim that Congress signaled an intent that the FTC Act does not apply to data security when it enacted more recent legislation addressing that field. As discussed below, the new legislation directs the FTC (and other agencies) to adopt specific data-security requirements in particular areas, grants the FTC streamlined rulemaking authority it would otherwise lack, and expands the range of available remedies. As the district court explained, this "subsequent data-security legislation seems to complement—*not preclude*—the FTC's authority" under the FTC Act. *Id*. 11 (JA12).

The district court next held that Wyndham had fair notice that it could be held liable under the FTC Act, just as it could be held liable under ordinary tort principles, if it unreasonably exposed consumers to harm by negligently handling their confidential data. Wyndham had argued that the FTC had not published rules or regulations detailing the data-security practices a company must adopt. The district court explained, however, that the FTC was not required to issue rules

governing data security before it could bring an enforcement action for unfair data-security practices. It found that Wyndham had adequate notice from the FTC's Business Guide and prior enforcement cases, which "constitute a body of experience and informed judgment to which courts and litigants may properly resort for guidance." *Opinion* 24 (JA25). Indeed, Wyndham's references on its website to "commercially reasonable" data-security practices indicated that the company understood the need to take reasonable data-security measures. *Id*.

Finally, the court held that the complaint "adequately pleads 'substantial injury to consumers'" necessary to state an unfairness claim. *Opinion* 26 (JA27). The agency "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." *Id*. at 27 (JA28). The court stressed that it was merely denying a motion to dismiss, not "render[ing] a decision on liability." *Id.* at 7 (JA8).

SUMMARY OF ARGUMENT

1. Consumers routinely provide businesses with sensitive information, including social security numbers, credit card information, and medical records. Once consumers turn such information over, they lose any ability to keep it secure. They must depend on merchants to take reasonable precautions to keep confidential personal data from falling into the wrong hands. This does not mean,

as Wyndham and its amici suggest, that the FTC deems any data breach to arise from an "unfair act or practice." As the Commission has explained, "the mere fact that such breaches occurred, standing alone, would not necessarily establish that [a company] engaged in 'unfair acts or practices.' … There is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution."[7] But that does not excuse businesses from greatly increasing the risk of data theft by ignoring basic security measures and unreasonably exposing sensitive consumer data to thieves. Such fundamental mistreatment of consumers is precisely the type of unfair practice that Congress enacted Section 5 to prohibit. Wyndham's contrary position would leave all consumers more vulnerable to data breaches and identity theft.

Although Congress did not foresee modern electronic commerce when it enacted the relevant provisions of the FTC Act, it understood that threats to consumer welfare would evolve as rapidly as the worlds of business and technology. It thus wrote Section 5 in open-ended terms, granting the FTC broad authority to pursue unfair practices across a broad range of economic contexts. Wyndham contends that a company cannot commit an "unfair act or practice"

---

[7] *In re LabMD, Inc.*, FTC Docket No. 9357, Order Denying LabMD's Motion to Dismiss, at 18 (Jan. 16, 2014) ("LabMD Order") (attached as an addendum to this brief) (appeal pending 11th Cir. No. 14-12144); *see also* 50th Settlement Statement, at 1.

unless it deliberately undertakes an "unscrupulous or unethical" course of action (Br. 20) and argues that unreasonably exposing consumers to third-party threats cannot qualify as "unfair." But this argument contradicts the statutory text and structure and collides with decades of contrary judicial precedent. *See*, *e.g.*, *FTC v. Neovi, Inc.*, 604 F.3d 1150 (9th Cir. 2010); *American Financial*, 767 F.2d 957. As that precedent confirms, a company can be liable for unfair practices if, like Wyndham, it unreasonably exposes consumers to substantial injury they cannot reasonably avoid, regardless of whether the company specifically intends the injury or whether intervening third-party wrongdoers are involved.

Wyndham is also wrong to argue that recent cybersecurity legislation "would be inexplicable if the Commission already had general substantive authority over this field." Br. 25. In fact, that legislation is consistent with the FTC's existing general authority and supplements it in several critical respects, which Wyndham ignores. Wyndham's reliance on *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000), is similarly misplaced. Unlike the FDA's attempt to regulate tobacco, which contradicted overwhelming evidence of contrary congressional intent, this FTC enforcement action comports fully with the FTC Act. In particular, it follows Congress's clear intent that the general statutory ban on unfair practices should apply to new types of consumer harm that Congress could not have foreseen in 1938.

Finally, the Commission determined earlier this year in *LabMD* that Section 5 applies to data-security lapses. That adjudicative ruling is entitled to *Chevron* deference. Wyndham opposes such deference on the sole ground that the agency's interpretation raises nondelegation concerns. But that nondelegation argument is meritless because, among other considerations, the criteria set forth in Section 5(n) plainly supply an "intelligible principle" for the exercise of agency discretion.

2. Wyndham also argues that this enforcement action violates due process because "the FTC has never provided any guidance" concerning reasonable data-security measures. Br. 35-36. That argument is untenable for multiple reasons.

First, under ordinary common-law negligence principles, businesses are always on notice that they must take commercially reasonable measures to protect consumers from foreseeable harm, whether or not the details of that responsibility are codified. Wyndham would have no fair-notice objection to a private tort suit alleging negligent data-security practices, and it likewise cannot plausibly object to this Section 5 suit, which alleges breach of the same duty of care.

Moreover, the FTC has in fact provided extensive guidance to industry concerning the elements of reasonable data security. Before the events at issue, the Commission found that a number of specific companies had acted unreasonably by failing to take many of the same data-security precautions that Wyndham neglected

here. It is irrelevant that those determinations appeared as part of consent decrees. Wyndham is complaining that the FTC failed to provide notice of its views on reasonable data security, and the consent decrees conveyed the agency's views whether or not they were reviewed by courts. In addition, the Commission's 2007 Business Guide identified basic precautions that companies should take to protect consumers. Again, Wyndham simply ignored many of these elementary precautions, to the detriment of its customers.

3. Finally, the FTC's complaint pleads sufficient facts to demonstrate "substantial injury" for purposes of Section 5(n). The complaint alleges several distinct forms of injury, including unreimbursed charges, impaired access to credit, and the time and money consumers wasted cleaning up the mess caused by Wyndham's repeated security lapses. Each of these allegations independently states a "substantial injury" that amply satisfies applicable pleading requirements.

ARGUMENT

I. A COMPANY'S FAILURE TO IMPLEMENT REASONABLE DATA-SECURITY PRACTICES CONSTITUTES AN "UNFAIR ACT OR PRACTICE"

A. Congress Deliberately Kept Section 5(a) Broad, Subject Only To The Cost-Benefit Analysis Of Section 5(n)

Section 5(a) of the FTC Act broadly prohibits, and authorizes the FTC to prevent, all "unfair … acts or practices in or affecting commerce." 15 U.S.C. § 45(a). In the Supreme Court's words, Congress "intentionally left development of the term 'unfair' to the Commission rather than attempting to define" any

specific practices. *Atlantic Refining*, 381 U.S. at 367 (quoting S. Rep. No. 63-597 at 13 (1914)). Congress had a "crystal clear" intent that the term should have "sweep and flexibility," *Sperry*, 405 U.S. at 241, and should remain "a flexible concept with evolving content," *FTC v. Bunte Bros., Inc.*, 312 U.S. 349, 353 (1941); *accord In re Smith*, 866 F.2d 576, 581 (3d Cir. 1989) ("[s]tatutes prohibiting unfair trade practices and acts have routinely been interpreted to be flexible and adaptable to respond to human inventiveness").

The evidence of that congressional intent is extensive. "When Congress created the Federal Trade Commission in 1914 and charted its power and responsibility…, it explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' … by enumerating the particular practices to which it was intended to apply." *Sperry*, 405 U.S. at 239-240 (citing S. Rep. No. 63-597 at 13); *see also* note 2 *supra* (describing relationship between "unfair methods" (1914) and "unfair practices" (1938) provisions). Thus, instead of "attempt[ing] to define the many and variable unfair practices which prevail in commerce and to forbid their continuance," Congress adopted "a general declaration condemning unfair practices" and "le[ft] it to the commission to determine what practices were unfair." S. Rep. 63-597 at 13. "[T]here were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others." *Id*. As the House Conference

Report put it, "[i]t is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." *American Financial*, 767 F.2d at 966 (quoting H.R. Rep. No. 63-1142 at 19 (1914) (Conf. Rep.)).

In short, Congress "expressly declined to delineate" the "particular acts or practices" deemed unfair, *American Financial*, 767 F.2d at 969, preferring instead to give the FTC "broad discretionary authority … to define unfair practices on a flexible and incremental basis," *id.* at 967. As a result, courts have "adopted a malleable view of the Commission's authority" to interpret and apply the term "unfair." *Id.* at 967-968. "Neither the language nor the history of the [FTC] [A]ct suggests that Congress intended to confine" the concept of unfairness to "fixed and unyielding categories." *FTC v. R.F. Keppel & Bro., Inc.*, 291 U.S. 304, 310 (1934). Of course "[t]he Commission's exercise of its unfairness authority in any particular instance is subject to judicial review," *American Financial*, 767 F.2d at 968, but courts extend "deference to the Commission's informed judgment that a particular commercial practice is to be condemned as 'unfair,'" *FTC v. Indiana Fed'n of Dentists*, 476 U.S. 447, 454 (1986).

With judicial approval, the FTC has invoked Section 5's prohibition on unfair practices against many disparate types of conduct that harm consumers with

no countervailing benefits. These practices have included not only outright fraud, but also breaching of contracts, *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354 (11th Cir. 1988), taking security interests in household goods, *American Financial*, 767 F.2d 957, commencing lawsuits against consumers in inconvenient forums, *Spiegel, Inc. v. FTC*, 540 F.2d 287 (7th Cir. 1976), and negligently failing to warn consumers of product defects, *Int'l Harvester Co.*, 104 F.T.C. at 1070.

Congress has limited the scope of the FTC's "unfairness" authority only once: in 1994, when it codified the 1980 *Policy Statement* by enacting Section 5(n) of the FTC Act. *See* pp.4-5, *supra.* Section 5(n) requires the Commission to consider not only a practice's harm to consumers, but also its possible benefits. Specifically, it provides that, in the consumer-protection context, the FTC may deem an act or practice unfair only if it "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 to competition." 15 U.S.C. § 45(n). That consumer injury test "is the most precise definition of unfairness articulated by either the Commission or Congress." *American Financial*, 767 F.2d at 972. Congress adopted no other restriction on the types of practices that fall within the prohibited category.

B. Wyndham's "Ordinary English" Argument Is Meritless

For the first time on appeal, Wyndham claims that, "[a]s a matter of ordinary English" as revealed in the dictionary, "the term 'unfair' cannot be stretched to encompass" a company's failure to adopt reasonable data-security practices. Br. 18, 20. According to Wyndham, this dictionary definition limits Section 5(a)'s prohibition to "unscrupulous or unethical behavior" that a company intentionally inflicts on its own customers. Br. 20-21. Wyndham waived this "ordinary English" argument by failing to raise it below, and for good reason: the argument is untenable.

As discussed, Congress, courts, and the Commission have applied Section 5 to ban "unfair practices" in disparate contexts over decades, and they have never suggested that the term should be limited as Wyndham proposes. That is reason enough to resist Wyndham's reliance on dictionary definitions as the principal source of statutory meaning, unmoored from historical practice. In any event, the dictionary affirmatively supports the Commission's interpretation. Like many common words, "unfair" encompasses several meanings. One is: "[c]ontrary to laws or conventions, especially in commerce." *American Heritage Dict. of the English Language* 1950 (3d ed. 1992). Companies that, like Wyndham, violate basic industry norms for protecting confidential consumer data are by definition

acting "[c]ontrary to [the] conventions" of reasonable business practices. *See also* § I.D, *infra* (addressing *Chevron* deference).[8]

Moreover, proper interpretation of Section 5(a) requires reference to statutory context. As the D.C. Circuit has recognized, Sections 5(a) and 5(n) should be read in tandem because "the consumer injury test," adopted by the Commission in 1980 and now codified in Section 5(n), "is the most precise definition of unfairness articulated by either the Commission or Congress." *American Financial*, 767 F.2d at 972. Like statutory prohibitions on "unjust" or "unreasonable" utility practices, *e.g.*, 47 U.S.C. §§ 201, 202, the "unfairness" prohibition of Section 5(a) is broad, enabling the Commission to "'prevent such acts or practices which injuriously affect the general public.'" *American Financial*, 767 F.2d at 966 (quoting H.R. Rep. No. 1613 at 3). And precisely because that authority is broad, Congress followed the FTC's own lead by

---

[8] Wyndham selectively quotes a different definition from another dictionary to argue that "an 'unfair' practice is one 'marked by injustice, partiality, or deception.'" Br. 18-19, quoting *Webster's Ninth New Collegiate Dictionary* 1288 (1988). But the same dictionary gives "not equitable" as a fully independent meaning of "unfair." *Id.* And one dictionary contemporaneous with the passage of the unfair practices provision lists "[r]easonable" and "equitable" as synonymous. *Webster's Second New International Dictionary* 865 (1934); *see id*. at 2773 (defining "unfair" to mean, *inter alia*, "not equitable in business dealings"). Yet another dictionary lists "unreasonable" as a synonym of "unfair" itself. Oxford Dictionaries (Oxford University Press), http://www.oxford dictionaries.com/us/definition/american_english/unfair (visited Nov. 4, 2014). Again, the core claim here is that Wyndham's data-security lapses were unfair to consumers because they were unreasonably harmful.

constraining that authority with—and *only* with—the cost-benefit analysis codified in Section 5(n). There is nothing "misguided," let alone "ironic" (Br. 21), about reading these two provisions together to understand this statutory scheme as a whole; that is how statutory interpretation is done. *See, e.g.*, *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997) ("The plainness or ambiguity of statutory language is determined by reference to the language itself, the specific context in which that language is used, and the broader context of the statute as a whole.").[9]

Indeed, unreasonably lax data-security practices present a case study in the proper application of Sections 5(a) and 5(n). In many settings, ranging from commercial transactions to financial dealings to medical care, consumers place their private data in the care of businesses. Once they have done so, they can no longer protect the data themselves. They instead have a legitimate expectation that the merchant itself will act reasonably to keep their private information safe. A merchant thwarts that expectation if, like Wyndham, it neglects basic data-security

[9] *LeBlanc v. Unifund CCR Partners*, 601 F.3d 1185 (11th Cir. 2010), cited by Wyndham (Br. 19), is inapposite. There, the Eleventh Circuit construed the phrase "unfair or unconscionable" in the Fair Debt Collection Practices Act and determined it to be as "vague as they come." *Id*. at 1200. The court then relied on a particular meaning of "unfair" that includes the concept of "deception," which was the relevant statutory concern in the deceptive debt-collection practice before the court. *Id.* & n.32. The court did not hold that "unfair" is limited to that meaning and did not address Section 5 of the FTC Act. Section 5 independently prohibits "deceptive acts or practices," so construing "unfair" to mean only "deceptive" would read the "unfairness" prong out of the statute.

conventions and unreasonably—*i.e.*, unfairly—places sensitive customer information at risk. In that case, the merchant "causes or is likely to cause substantial injury to consumers," 15 U.S.C. § 45(n), in the form of monetary loss, identity theft, and countless hours spent trying to mitigate the damage, among other harms. Such injuries are not "reasonably avoidable by consumers themselves" because, as discussed, consumers lose control over their personal information once they turn it over to merchants. *Id.* And Wyndham does not even argue that such harm is "outweighed by countervailing benefits to consumers or to competition." *Id.*

Wyndham further contradicts decades of precedent when it proposes (on the sole basis of its preferred dictionary definition) to confine the statutory prohibition to acts undertaken with "unscrupulous or unethical" intent. Br. 20-21.[10] The Commission rejected any such requirement in the 1980 *Policy Statement*, explaining that "the theory of immoral or unscrupulous conduct was abandoned altogether" as an independent basis of liability in assessing whether a company's practices were "unfair." 104 F.T.C. at 1061 n.46. Applying the *Policy Statement*, the Commission held in *International Harvester* that a company's *negligent* failure

[10] It is doubtful that Wyndham would even benefit from this proposed limitation on Section 5 liability. Wyndham behaved "unethically" by betraying consumers' trust that it would take reasonable measures to protect their financial data.

to notify consumers about hazards in its product constituted an unfair act or practice even in the absence of "a deliberate act on the part of the seller." 104 F.T.C. at 1059. When Congress codified the *Policy Statement* a decade later, it too chose not to impose any heightened scienter requirement in unfairness cases. Wyndham may not add new terms of its choosing to the statute.

Courts have also consistently held that, in the Ninth Circuit's words, "consumers are injured for purposes of the Act not solely through the machinations of those with ill intentions, but also through the actions of those whose practices facilitate, or contribute to, ill intentioned schemes if the injury was a predictable consequence of those actions." *Neovi*, 604 F.3d at 1156. The Eleventh Circuit similarly held in *Orkin* that a breach of contract could constitute an unfair practice, whether or not it "involve[d] some sort of deceptive or fraudulent behavior." 849 F.2d at 1363. And the D.C. Circuit held in *American Financial* that Section 5 is not limited to "conduct involving deception, coercion or the withholding of material information." 767 F.2d at 982; *see also id*. ("it is not for this court to step in and confine, by judicial fiat, the Commission's unfairness authority to acts or practices found to be deceptive or coercive"); *FTC v. Algoma Lumber Co.*, 291 U.S. 67, 79 (1934) (holding that anticompetitive "motives" are not an element of liability for an unfair method of competition).

Wyndham likewise contradicts decades of precedent when it argues (again on the sole basis of its chosen dictionary definition) that a company's acts can be unfair only if they directly injure consumers and not if they unreasonably enable third parties to harm consumers. Br. 20-21. As both the Supreme Court and this Court have held, a business can be liable under Section 5 even if it merely "furnishes another with the means of consummating a fraud." *FTC v. Winsted Hosiery Co.*, 258 U.S. 483, 494 (1922); *accord Regina Corp. v. FTC*, 322 F.2d 765, 768 (3d Cir. 1963) ("[o]ne who places in the hands of another a means of consummating a fraud … is himself guilty of a violation of the [FTC] Act") (quotation marks and citation omitted).

In *Neovi*, for example, the Ninth Circuit held that a defendant can be liable for "unfair practices" even though its own actions merely "facilitated fraud" and the ultimate harm to consumers flowed from "the contribution of independent causal agents." 604 F.3d at 1155. The defendant in that case offered a service enabling users to create checks drawn on bank accounts, but failed to institute safeguards to ensure that account owners had authorized payment of such checks. Thieves used the service to make fraudulent withdrawals. Like Wyndham here, the defendant argued that it committed no unfair practice because it did not itself perpetrate fraud on consumers; instead, it protested, it was guilty only of creating a service that third parties misused. The court rejected this argument on the ground

that it "ignores the fact that [the defendant] created and controlled a system that facilitated fraud and that the company was on notice as to the high fraud rate." *Id*. at 1155. It added: the "absence of deceit is not dispositive. Nor is actual knowledge of the harm a requirement under the Act." *Id*. at 1156. Similarly here, Wyndham created and controlled a computer network that collected private data, yet it repeatedly failed to take reasonable steps to protect that network against data theft, even after its system was repeatedly breached. Wyndham's "third party wrongdoer" rationale for avoiding liability would contradict the central holding of *Neovi*.[11]

Finally, Wyndham protests that "any injury to consumers is derivative of the injury to [Wyndham] itself" and that Wyndham "certainly ha[d] no incentive to tolerate … crimes against itself." Br. 21. But Sections 5(a) and 5(n) contain no exemption for a business that exposes itself to harm through negligence at the same time that it injures consumers. The very premise of commercial liability for negligence is that a company's incentives to take reasonable precautions to protect

[11] As in *Neovi*, the Commission often brings unfairness enforcement actions against defendants that may not themselves have intended to harm consumers but that unreasonably exposed consumers to harm inflicted by third parties. For example, the agency recently brought "cramming" cases alleging that mobile phone companies, which acted as billing conduits, unreasonably enabled third parties to place fraudulent charges on customer bills for services that customers did not order. *See FTC v. T-Mobile USA, Inc.*, No. 2:14-cv-967 (W.D. Wash.) (complaint filed July 1, 2014); *FTC v. AT&T Mobility, LLC*, No. 1:14-cv-3227 (N.D. Ga.) (complaint and proposed stipulated order filed Oct. 8, 2014).

consumers are poorly aligned with the interests of consumers themselves, as were Wyndham's here.

C. Recent Cybersecurity Legislation Supplements, Rather Than Displaces, FTC Authority Under Section 5

Wyndham next argues that various recent cybersecurity statutes preclude the inference that Congress thought the FTC could use its Section 5 authority to address cybersecurity. According to Wyndham, these statutes "would be inexplicable if the Commission already had general substantive authority over this field." Br. 25. That is wrong for reasons that the district court explained, *Opinion* 10-12 (JA11-13), and Wyndham largely ignores.

In several substantive and procedural respects, the recent legislation supplements the FTC's general authority to proceed under Section 5 against unreasonably lax data-security measures as unfair practices. First, the laws give the Commission streamlined *rulemaking* authority it otherwise lacks under the FTC Act. For example, the Gramm-Leach-Bliley Act ("GLBA"), 113 Stat. 1338 (1999), the Fair Credit Reporting Act ("FCRA"), 117 Stat. 1952 (2003), and the Children's Online Privacy Protection Act of 1998 ("COPPA"), 112 Stat. 2681, all enable the Commission to adopt data-protection rules using notice-and-comment rulemaking procedures under the Administrative Procedure Act. 15 U.S.C. § 1681s(a)(1) (FCRA); 15 U.S.C. § 6804(a)(1) (GLBA); 15 U.S.C. § 6502(b) (COPPA). In the absence of that APA authority, any Commission rulemaking

proceedings in this area would be subject to the cumbersome (and thus rarely used) Magnuson-Moss procedures, which require full-blown evidentiary hearings and witness testimony. *See* 15 U.S.C. § 57a.

Second, the recent legislation augments the *remedies* the Commission can seek in data-security enforcement actions. For example, the FCRA and COPPA empower the Commission to seek civil penalties, whereas the FTC Act generally entitles the FTC to pursue only equitable remedies. 15 U.S.C. § 1681s(a)(2) (FCRA); 15 U.S.C. § 6505(d) (COPPA); *compare* 15 U.S.C. §§ 45(b), 53(b) (FTC Act).

Third, all three statutes authorize the FTC to obtain relief even when it cannot demonstrate substantial consumer injury. 15 U.S.C. § 1681s(a) (FCRA); 15 U.S.C. §§ 6801(b), 6805(a)(7) (GLBA); 15 U.S.C. § 6505(d) (COPPA).

Fourth, the more recent legislation affirmatively *requires* the FTC (and other agencies) to address policy concerns in specific areas where the FTC already had *discretionary* authority to act. Congress commonly authorizes agencies to oversee entire fields and later specifies, in a few areas, minimum steps those agencies must take in exercising that authority. Such legislation does not detract from the agencies' broader authority. *See*, *e.g.*, *Cablevision Sys. Corp. v. FCC*, 649 F.3d 695, 705-706 (D.C. Cir. 2011).

In all of these respects, the subsequent laws supplement the FTC's preexisting authority, as the district court recognized. *Opinion* 11 (JA12); *see also LabMD Order* 9-13. There is thus no basis for Wyndham's suggestion that these laws somehow "presuppose the absence … of pre-existing substantive authority in this area." Br. 26.

For similar reasons, this case bears no resemblance to *Brown & Williamson*, 529 U.S. at 125, on which Wyndham heavily relies. There, the Supreme Court held that the Food and Drug Administration lacked authority to regulate tobacco under the Food, Drug, and Cosmetic Act because the exercise of authority under that general statute would have contradicted more recent statutes pertaining specifically to tobacco. For example, the Court observed that, if the FDA had such jurisdiction, its own findings would have forced it to prohibit tobacco products altogether, thereby clashing with tobacco-specific statutes confirming that Congress did *not* wish to ban such products. *See id*. at 137-39. That and other statutory conflicts indicated Congress's intent to "clearly preclude[] the FDA from asserting jurisdiction to regulate tobacco products." *Id*. at 126. In contrast, Wyndham "can cite no similar congressional intent to preserve inadequate data-

security practices that unreasonably injure consumers." *LabMD Order* at 6; *accord Opinion* 10 (JA11).[12]

The *Brown & Williamson* Court also found it "extremely unlikely that Congress could have intended to place tobacco within the ambit of the FDCA absent any discussion of the matter," given "the economic and political significance of the tobacco industry at the time." 529 U.S. at 147. No corresponding inference could be drawn here. When Congress enacted the prohibition on unfair practices in 1938, it obviously could not have anticipated the "economic and political significance" of data-security practices in the modern digital economy, and thus could not have intended to keep the FTC from addressing those practices. To the contrary, Congress intended to delegate broad authority to the FTC to address emerging business practices, including those that were unforeseeable when the statute was enacted. *See* Section I.A, *supra.*

Absent an affirmative conflict between the FTC Act and the more recent statutes, Wyndham's reliance on those statutes for evidence of congressional intent

---

[12] Wyndham's reliance on *Util. Air Regulatory Grp. v. EPA*, 134 S. Ct. 2427 (2014), is likewise unfounded. There, EPA's interpretation of its organic act was "inconsistent with—in fact, would overthrow—the Act's structure and design," *id*. at 2442, and would be "incompatible" with "the substance of Congress' regulatory scheme," *id*. at 2443 (citing *Brown & Williamson*, 529 U.S. at 156). Indeed, EPA itself acknowledged that its interpretation "would render the statute 'unrecognizable to the Congress that designed' it." 134 S. Ct. at 2445. The opposite is true here

underlying the FTC Act falls flat. As the Supreme Court has explained, "later enacted laws" have little interpretive value where, as here, they "do not declare the meaning of earlier law," "do not seek to clarify an earlier enacted general term," "do not depend for their effectiveness upon clarification, or a change in the meaning of an earlier statute," and "do not reflect any direct focus by Congress upon the meaning of the earlier enacted provisions." *Almendarez-Torres v. United States*, 523 U.S. 224, 237 (1998) (citations omitted). In such circumstances, subsequent legislation cannot be used as a "forward looking legislative mandate, guidance, or direct suggestion about how courts should interpret the earlier provisions." *Id*.[13]

Wyndham cites no case to the contrary. Every precedent on which it relies (Br. 25-26) involved a later-enacted statute that *conflicted* with the earlier statute. In *United States v. Fausto*, 484 U.S. 439 (1988), for example, the Court held that preservation of a prior statutory interpretation "would undermine" more recent legislation. *Id*. at 451. Even then, the Court took pains to point out that "it can be strongly presumed that Congress will specifically address language on the statute books that it wishes to change." *Id*. at 453. Similarly, *United States v. Estate of*

[13] In contrast, as discussed above, Section 5(n) *does* cast strong interpretive light on Section 5(a) because Congress enacted that provision for the express purpose of clarifying the Commission's discretion under Section 5(a). *See* Section I.B, *supra.*

Romani, 523 U.S. 517 (1998), involved a "plain inconsistency" between statutes. *Id*. at 520. Wyndham improperly relies (Br. 26) on an out-of-context quote from *Romani* that addresses the construction of otherwise irreconcilable statutes, and not statutes that (like those here) are consistent. The maxim that a court must "make sense rather than nonsense" of the law, Br. 26, quoting *W. Va. Univ. Hosps., Inc. v. Casey*, 499 U.S. 83, 101 (1991), applies only when statutes conflict.

This case more closely resembles *Massachusetts v. EPA*, 549 U.S. 497 (2007). There, the Supreme Court read the Clean Air Act broadly to cover carbon dioxide emissions as "air pollutants" despite subsequent legislation addressing climate change. The Court distinguished *Brown & Williamson* on the ground that the later acts do not "conflict[] in any way" with the earlier statute and thus provided no basis to narrow the existing law. *Id*. at 531. Similarly here, Wyndham cannot "explain how the FTC's unfairness authority over data security would lead to a result that is incompatible with" data-security statutes later passed by Congress. *Opinion* 10 (JA11).

It is also immaterial that Congress has recently considered, but has not enacted, legislation that would grant the FTC new remedial tools and would direct it, among other things, to promulgate general rules covering data security. Br. 29-30. Those unenacted bills, like the statutes Congress actually did pass, merely would have *supplemented* the FTC's existing Section 5 authority and thus would

not have cast doubt on that authority even had they been enacted. Equally important, "a proposal that does not become law" is "a particularly dangerous ground on which to rest an interpretation of a prior statute." *Pension Benefit Guar. Corp. v. LTV Corp.*, 496 U.S. 633, 650 (1990). "Congressional inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction including the inference that the existing legislation already incorporated the offered change." *Id*. (quotation marks and citation omitted); *accord In re Visteon Corp.*, 612 F.3d 210, 230-231 (3d Cir. 2010); *see United States v. Southwestern Cable Co.*, 392 U.S. 157, 170 (1968) (failed requests for legislation do not prove agency "did not already possess" authority). Indeed, several of the bills included savings clauses to preserve the FTC's existing data-security authority. *See* S. 1207, 112th Cong. § 6(d) (1st Sess. 2011); H.R. 2577, 112 Cong. § 6(d) (1st Sess. 2011); H.R. 1841, 112 Cong. § 6(d) (1st Sess. 2011); H.R. 1707, 112 Cong. § 6(d) (1st Sess. 2011).

There similarly is no merit to Wyndham's claim that "the Commission's interpretation of Section 5 is inconsistent with its repeated efforts to obtain from Congress the very authority it purports to wield here." Br. 28-29. Wyndham cites the testimony of FTC officials in support of legislation that would give the Commission new powers in the data-security area. But that testimony contradicts Wyndham's argument. As those officials explained, such new legislation would

usefully *supplement* the FTC's existing data-security authority. The officials nowhere suggested that the FTC currently lacks such authority and needs legislation to fill the void.[14]

D. The Commission's Interpretation of Section 5 Is Entitled To *Chevron* Deference

Earlier this year, the Commission addressed these same statutory-authority issues in an administrative proceeding involving LabMD, a medical-testing company charged with insufficiently protecting patient medical records from hackers. LabMD, like Wyndham here, asserted that inadequate data-security measures cannot constitute "unfair practices" under Section 5. Sitting in its capacity as an administrative tribunal, the Commission rejected that claim, unanimously determining that its "authority to protect consumers from unfair practices relating to deficient data security measures is well-supported by the FTC Act." *LabMD Order* 3.

The Commission's determination that its authority under the "unfair practices" provision of Section 5 extends to data-security practices is entitled to

---

[14] For example, Commissioner (now Chairwoman) Ramirez referred to "the FTC Act's proscription against unfair or deceptive acts or practices in cases … where [a business's] failure to employ reasonable security measures causes or is likely to cause substantial consumer injury." 2011 WL 2358081 (June 15, 2011). David Vladeck, then-Director of the Bureau of Consumer Protection, testified that unfairness authority extends to "cases where … [a] failure to employ reasonable security measures causes or is likely to cause substantial consumer injury." 2011 WL 1971214 (May 4, 2011).

substantial deference. "Where the Congress has provided that an administrative agency initially apply a broad statutory term to a particular situation, [the reviewing court's] function is limited to determining whether the Commission's decision has warrant in the record and a reasonable basis in law." *Atlantic Refining*, 381 U.S. at 367 (quotation marks and citation omitted). Specifically, under *Chevron*, if "Congress has not directly addressed the precise question at issue," and if "the agency's answer is based on a permissible construction of the statute"—as it is here—a reviewing court must yield to that construction. *Chevron*, 467 U.S. at 842-843. The Supreme Court recently confirmed "that *Chevron* applies to cases in which an agency adopts a construction of a jurisdictional provision of a statute it administers," *City of Arlington, Tex. v. FCC*, 133 S. Ct. 1863, 1871 (2013), and reaffirmed that deference extends to agency adjudicatory decisions that, like *LabMD*, are issued pursuant to statutory authority, *id*. at 1874.

In response, Wyndham does not argue that Congress has "directly addressed the precise question at issue" or that deference is unwarranted under *Chevron* "Step One." Instead, Wyndham asserts only that Section 5 must be construed narrowly to avoid "a serious non-delegation question" (Br. 34) and that this "doctrine of constitutional avoidance" trumps any deference due to agency statutory interpretations (Br. 32). But the constitutional-avoidance canon applies

only where an agency's interpretation poses "serious" constitutional concerns. *See, e.g.*, *Verizon Commc'ns v. FCC*, 535 U.S. 467, 523 (2002). Wyndham's nondelegation argument is simply implausible, which likely explains why Wyndham did not raise it below.

As this Court has recognized, "[u]nder modern application of the nondelegation doctrine, as long as Congress 'lay[s] down by legislative act an intelligible principle to which the person or body authorized to exercise the delegated authority is directed to conform, such legislative action is not a forbidden delegation of legislative power.'" *United States v. Cooper*, 750 F.3d 263, 270 (3d Cir. 2014) (quoting *Mistretta v. United States*, 488 U.S. 361, 372 (1989)). Indeed, the Supreme Court "has not invalidated a statute for violating the nondelegation doctrine in … nearly 80 years," despite the passage of statutes more open-ended than Section 5. *Id*. For example, Congress has authorized the FCC to police "just and reasonable rates," 47 U.S.C. § 201(b), and to grant licenses pursuant to the "public interest," 47 U.S.C. § 307(a), and it has authorized the National Labor Relations Board to determine whether employers have engaged in "good faith" collective bargaining, 29 U.S.C. § 158(d). No one today seriously suggests that these open-ended standards violate the nondelegation rule. Not surprisingly, Section 5 itself "has withstood repeated attack on delegation grounds." *Int'l Harvester*, 104 F.T.C. at 1068 & n.67 (citing *Nat'l Harness Mfrs.' Ass'n v. FTC*,

268 F. 705 (6th Cir. 1920); *Sears, Roebuck & Co. v. FTC*, 258 F. 307, 312 (7th Cir. 1919); and *T.C. Hurst & Son v. FTC*, 268 F. 874 (E.D. Va. 1920)).

Here, Congress has confined unfairness cases to those that satisfy the three criteria of Section 5(n). That is a clearer and more specific "intelligible principle" than others found in the many statutory schemes that courts have deemed constitutional, and by itself it refutes Wyndham's new-found nondelegation concern. Section 5(n) similarly undermines Wyndham's argument that the FTC's construction of Section 5 contains no "limiting principle." Br. 22. The cost-benefit test of Section 5(n) supplies Congress's choice of limiting principles, and Wyndham identifies no basis for reading new ones into the statute.

II. WYNDHAM HAD FAIR NOTICE OF ITS OBLIGATION TO TAKE REASONABLE STEPS TO PROTECT CONFIDENTIAL CONSUMER DATA

Wyndham claims that it has been denied due process because "the FTC has never provided any guidance" as to what data-security practices Wyndham should have implemented. Br. 35-36. That argument is untenable for two independent reasons. First, the standard of care the FTC is enforcing here reflects basic negligence principles. All companies are on notice that, even in the absence of specific written guidance, they must follow commercially reasonable standards of care. Second, the FTC has warned industry repeatedly to take the basic data-security precautions that Wyndham ignored here.

A. All Companies Have Notice Of Their Obligation To Follow Basic Standards Of Care

The FTC's complaint charges Wyndham with violating a duty to act reasonably in the face of known data-security threats. That duty of care is rooted as much in common-law negligence principles as in the FTC Act. All businesses operate under the knowledge that they must act reasonably towards consumers and that a failure to do so can result in tort liability. Hotels in particular have a duty of care to "take reasonable action to protect" their guests from harm. Restatement (Second) of Torts § 314A (1965). Moreover, when Wyndham received confidential information entrusted to it by its customers, it effectively acted in the position of a bailee, which must "exercise reasonable and ordinary care" in protecting the property it has accepted from a bailor. *Am. Enka Co. v. Wicaco Mach. Corp.*, 686 F.2d 1050, 1053 (3d Cir. 1982) (citations omitted).

Wyndham is no more entitled to detailed written guidance when it is sued by the FTC for unreasonably exposing consumers to harm than it would be if sued by private plaintiffs who have suffered harm as a result of the same unreasonable conduct. As the Commission explained in the *LabMD Order*, "[e]very day, courts and juries subject companies to tort liability for violating uncodified standards of care, and the contexts in which they make those fact-specific judgments are as varied and fast-changing as the world of commerce and technology itself." *Id*. at 17; *see Opinion* 22 (JA23) (tort liability "is routinely found for unreasonable

conduct without the need for particularized prohibitions").[15] For example, doctors are often held liable in medical malpractice cases for violating uncodified standards of care that are established only in after-the-fact expert testimony.

Moreover, when factfinders in tort cases find that corporate defendants have violated an unwritten rule of conduct, they "can normally impose compensatory and even punitive damages," whereas the FTC is generally confined to equitable remedies. *LabMD Order* 16. Despite the broad relief available to private plaintiffs, no one would contend that a trial court violates fair notice principles when, by applying ordinary duty-of-care principles, it finds that a commercial defendant has acted negligently by inadequately safeguarding consumers.

Duties to act "reasonably" and to follow similarly general standards of conduct are ubiquitous in statutory law as well. To name just a few: Restraints of trade under the Sherman Act are often assessed under a fact-specific "rule of reason," *see Leegin Creative Leather Prods., Inc. v. PSKS, Inc.*, 551 U.S. 877, 899 (2007), yet violations are subject to automatic treble damages. The FCC polices the obligation of common carriers to offer "just and reasonable" rates and terms of

---

[15] Commissioner Joshua Wright wrote the unanimous opinion in *LabMD*, which rejected a fair-notice argument identical to Wyndham's. Wyndham's reliance (Br. 38) on an article written by Commissioner Wright to support its argument that the Commission has provided too little guidance in this area thus is misplaced. That article addressed Section 5's antitrust-oriented prohibition on "unfair *methods of competition*," to which the limitations of Section 5(n) do not apply.

service. 47 U.S.C. § 201(b). Occupational safety regulations use a reasonable-person test to assess the adequacy of safety precautions. *Voegele Co., Inc. v. OSHRC*, 625 F.2d 1075, 1078-1079 (3d Cir. 1980). In all of those contexts, companies can be subject to sanctions under guideposts no more specific than Section 5.

Wyndham's claims of surprise ring particularly hollow in light of its longstanding assurances to customers that it would in fact provide reasonable data security. Wyndham's privacy policy assured customers that Wyndham "safeguard[s] … [c]ustomers' personally identifiable information by using industry standard practices," including "*commercially reasonable* efforts to make … collection of such [i]nformation consistent with all applicable laws and regulations." Cmplt. ¶21 (JA64) (emphasis added). The company promised to "utilize a variety of different security measures designed to protect" customer information, such as encrypting data, as well as "commercially reasonable efforts to create and maintain 'fire walls' and other appropriate safeguards" to protect private customer data. *Id*. Those are some of the very precautions that the FTC alleges Wyndham did *not* take. Having promised that it would take these precautions, Wyndham can hardly claim that it lacked notice of its responsibility to do so.

Wyndham barely responds to any of these points. It argues only that "common law cannot resolve the fair-notice issue here" because "liability under the FTC Act is not bounded by the common law." Br. 40 (citing *Sperry*, 405 U.S. at 240-244). But it is immaterial that common law principles do not limit the FTC's authority under Section 5 as a general matter. In the complaint challenged here, the Commission is relying on a standard of care rooted firmly in common law principles of negligence; indeed, the Section 5(n) factors parallel the basic considerations that inform tort liability under the same circumstances. Thus, even apart from the FTC-specific guidance discussed below, those background common law principles, acknowledged by Wyndham in its data security policy, provided constitutionally adequate notice of a duty under the FTC Act. That the FTC's authority may extend beyond the boundaries of the common law in other respects does not mean that Wyndham lacked constitutionally adequate notice of a duty to act reasonably in accordance with generally applicable standards of reasonable behavior.

B. The FTC Has Repeatedly Advised Industry To Adopt The Basic Data-Security Measures That Wyndham Failed To Implement

Even apart from the duty of reasonable care that all businesses must follow, the FTC has provided constitutionally adequate notice to Wyndham by repeatedly and publicly advising companies to undertake the basic data-security precautions that Wyndham failed to take.

Agencies have broad discretion in choosing how to provide "a sufficient, publicly accessible statement" of a regulatory requirement. *Secretary of Labor v. Beverly Healthcare-Hillview*, 541 F.3d 193, 202 (3d Cir. 2008) (citing *United States v. Lachman*, 387 F.3d 42, 57 (1st Cir. 2004)). In *Star Wireless, LLC v. FCC*, 522 F.3d 469, 474 (D.C. Cir. 2008), for example, the D.C. Circuit held that public announcements sufficiently notified parties of applicable regulatory requirements. *Accord Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995) ("public statements" can satisfy notice requirement); *Abhe & Svoboda, Inc. v. Chao*, 508 F.3d 1052, 1060 (D.C. Cir. 2007) (administrative decisions sufficed). Here, the FTC gave the public—including Wyndham—ample notice of its data-security obligations in two different ways: through a series of administrative decisions finding specific companies liable for inadequate data-security practices, and through the publication of the Business Guide in 2007.

1. The Commission's Complaints and Consent Judgments Identified The Basic Data-Security Obligations That Wyndham Neglected

Beginning in 2005, the Commission has issued numerous complaints and consent decrees charging companies with violating Section 5 for unreasonable reasonable data-security practices. *See* pp.7-8 and notes 4 & 5, *supra*. The complaints make clear that the failure to take reasonable data-security measures may constitute an unfair practice, and they flesh out the types of security lapses that may be deemed unreasonable. The Commission publishes these materials on

its website, provides notice in the Federal Register, and solicits and responds to public comment in order to take into account the views of relevant stakeholders and ensure that it has complete information on evolving technologies and other developments.

Given these widely available materials, Wyndham cannot seriously contend that it lacked notice that its security failures—comparable to those committed by other companies against which the FTC has taken action—could trigger Section 5 liability. The 2005 complaint in *BJ's Wholesale Club*, for example, charged that the company engaged in unfair acts by "fail[ing] to employ reasonable and appropriate security measures to protect personal information" because it did not encrypt data, change default passwords, detect intrusions, or conduct security investigations. 140 F.T.C. at 467. Wyndham later failed to take those very precautions. The complaint in *DSW, Inc.*, published later that year, alleged failure to detect unauthorized access, and failure to use adequate password security. *See* http://www.ftc.gov/sites/default/files/documents/cases/2005/12/051201comp0523096.pdf. The complaint in *TJX* charged unfair practices for inadequately secure passwords, inadequate use of firewalls, failure to encrypt data, and failure to install software security patches. *See* http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080327complaint_0.pdf. The other complaints (*see* notes 4 & 5, *supra*) similarly alleged unreasonable practices premised on similar specific

failures, many of which parallel Wyndham's lapses. The district court was correct when it held that these complaints "constitute a body of experience and informed judgment" to which companies holding private data "may properly resort for guidance." *Opinion* at 24 (JA25).

Wyndham erroneously argues that "the complaints fail to spell out what specific cybersecurity practices … actually triggered the alleged violation." Br. 42. In fact, as the *BJ's* example illustrates, the complaints specify the alleged unreasonable practices in some detail.[16] Each complaint gives the business community further information about the types of security lapses that can trigger Section 5 liability. And Wyndham committed virtually every security lapse described in the prior complaints. It cannot now claim that it did not know what was expected of it.

Wyndham gains nothing by contending that these materials do not specify exactly "what firewall configurations," "encryption techniques," or "password requirements" companies should adopt as reasonable measures to protect consumers against evolving threats. Br. 37. Wyndham is not charged with using 12-character passwords when it could have used 13-character ones. Its lapses are

[16] Of the nine FTC data-security judgments issued before Wyndham's first data breach, *see* notes 4 & 5, *supra*, five of them—*BJ's*, *DSW*, *CardSystems*, *TJX*, and *Reed Elsevier*—involved "unfair practices" claims. Although the other four involved claims of "deceptive practices" or other statutory violations, a core allegation in each case was that specific data-security failures were unreasonable.

much more basic, akin to using "password" as the password. Among them: Wyndham used no firewalls at critical points in its network; it did not encrypt credit card data on property management servers; and it failed to change manufacturer default passwords. *See*, *e.g.*, Cmplt. ¶24(f) (JA66-67) ("For example, to allow remote access to a hotel's property management system, which was developed by software developer Micros Systems, Inc., Defendants used the phrase 'micros' as both the user ID and the password[.]"). Wyndham cannot complain that it lacked specific guidance on the fine details of implementing basic precautions that it failed to take at all.

Finally, Wyndham argues that prior complaints against other companies "do[] not and cannot provide fair notice" when they are resolved by consent judgments because such dispositions do not "adjudicate the legality of any action." Br. 41. That is beside the point. The issue here is not whether Wyndham violated consent decrees entered by other companies. Rather, the pertinent question is whether, as Wyndham alleges, the FTC provided insufficient guidance as to what data-security measures companies should undertake. The Commission's complaints and consent judgments provide considerable guidance on the types of gaps in corporate data-security programs that are likely to result in consumer harm and FTC enforcement action. Moreover, these are precisely the type of administrative materials that, as the Supreme Court has recognized, parties may

"properly resort to for guidance." *Gen. Elec. Co. v. Gilbert*, 429 U.S. 125, 142 (1976) (citation and alteration omitted). Due process requires no more.

2. The 2007 Business Guide Identified The Basic Data-Security Obligations That Wyndham Failed To Satisfy

In addition to the complaints against specific company practices, Wyndham also had notice through the Commission's efforts to educate the business community about data-security practices. In 2007, before the first infiltration of Wyndham's network, the FTC issued the "Guide for Business" on "Protecting Personal Information," which provided a catalogue of reasonable data-security practices. *See* pp.5-6, *supra.*

The Guide specifically cautioned companies against nearly all of the basic data-security lapses that Wyndham later committed. First, it emphasized the importance of "[i]dentify[ing] the computers or servers where sensitive personal information is stored" and "all connections to the computers where you store sensitive information." Business Guide 9. Wyndham did not take those steps, which facilitated the infiltration of its network. Cmplt. ¶24(a), (g), & (j) (JA66-67). The Guide advised companies to "consider encrypting sensitive information that is stored on your computer network." Business Guide 10. Wyndham did not encrypt its customers' credit card information, which enabled thieves to use it more easily once they stole it. Cmplt. ¶24(b) (JA65). The Guide warned that "[w]hen installing new software, immediately change vendor supplied default passwords to

a more secure strong password." Business Guide 13. Wyndham allowed computers on its network to use default passwords, leaving the network more vulnerable to intrusion. Cmplt. ¶24(e) & (f) (JA66-67). The Guide recommended that companies "implement policies for installing vendor-approved patches to correct [security] problems." Business Guide 10. Property management systems controlled by Wyndham used out-of-date software that could not receive security patches, again leaving its system undefended. Cmplt. ¶24(d) (JA66).

The Business Guide further advised that computer networks "[u]se a firewall to protect your computer from hacker attacks while it is connected to the Internet," and, where "some computers on your network store sensitive information while others do not, consider using additional firewalls to protect the computers with sensitive information." Business Guide 15. Wyndham did not use firewalls at critical points in its network, so once hackers gained access to one network computer, they could steal customer data from others. Cmplt. ¶24(a) (JA65). Finally, the Guide suggested that in the event of a security breach, a company should "consider using an intrusion detection system," Business Guide 15, and should "[k]eep an eye out for activity from new users, multiple log-in attempts from unknown users or computers," *id*. at 16. Wyndham ignored that advice too, also to its customers' detriment. Cmplt. ¶24(h)-(j) (JA67).

In short, well before the breaches that resulted in the theft of Wyndham's customer data, the FTC had provided considerable guidance on the elements of commercially reasonable data-security measures. The Business Guide provided guidance on virtually every security lapse that Wyndham subsequently committed.

Wyndham asserts that the Guide "contains little specific guidance on any particular cybersecurity practices." Br. 43. As discussed, however, the Business Guide, though short, contains quite specific guidance on data-security practices. Wyndham ignores that guidance in its brief, just as it did in running its computer operations. Of course, the Guide did not specify exactly what exact *types* of firewalls, encryption algorithms, intrusion-detection systems, or password protocols companies should use to meet evolving security threats. But that fact cannot help Wyndham, which clearly had notice that any prudent company must implement at least *some* firewall protection at critical network points, *some* encryption of sensitive data, *some* intrusion-detection systems, and *some* reasonably protective password requirements.

Finally, Wyndham objects that the Business Guide provided inadequate notice that failure to implement such basic data-security safeguards could subject a company to Section 5 liability. That objection makes little sense, both because the Guide warns explicitly that "the Federal Trade Commission Act may require you to provide reasonable security" of the types described within, Business Guide 5,

and, more fundamentally, because the Commission had already based liability in *BJ's* and other unfair-practices cases on failure to implement such safeguards.[17]

III. WYNDHAM'S CHALLENGE TO THE SUFFICIENCY OF THE FACTUAL PLEADINGS LACKS MERIT

As discussed, a company is liable under Section 5 for unfair acts or practices that, *inter alia*, cause "substantial injury" that is "not reasonably avoidable by consumers themselves." 15 U.S.C. § 45(n).[18] Wyndham contends that the complaint "fails to plead any *facts*" that satisfy those two statutory criteria. Br. 46. That challenge is meritless.

A complaint need not contain "detailed factual allegations" to meet the applicable pleading requirements of Rule 8(a) of the Federal Rules of Civil Procedure. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). Rather, the complaint "must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). A claim is plausible "when the plaintiff

---

[17] Wyndham argued below that due process requires the Commission to promulgate rules before it may undertake enforcement actions. Wyndham abandons that argument now. Br. 39. The argument is meritless anyway for the reasons the FTC explained below and the district court adopted. *Opinion* 18-22 (JA19-23). *See SEC v. Chenery*, 332 U.S. 194, 202-203 (1947); *Voegele*, 625 F.2d 1075.

[18] Section 5(n) also specifies that there be no "countervailing benefits to consumers or competition" sufficient to outweigh a practice's harmful effects. Wyndham does not challenge the sufficiency of the complaint's allegations concerning that criterion.

pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 550 U.S. at 678.

The complaint here amply meets that standard. It alleges the following facts: Wyndham's failure to implement reasonable and appropriate security measures led to three distinct data breaches that compromised more than 619,000 credit and debit card numbers. *See* Cmplt. ¶40 (JA72-73). The hackers exported that confidential information to Russia and enabled its use to place more than $10 million in fraudulent charges on the accounts of Wyndham's customers. *Id.* Consumers consequently suffered several distinct injuries, including "unreimbursed fraudulent charges, increased costs, and lost access to funds or credit" and "expend[iture of] time and money resolving fraudulent charges and mitigating subsequent harm." *Id.* The complaint thus pleads several distinct and unavoidable consumer harms, each of which independently meets the Commission's pleading burden.

A. The Allegation That Customers Incurred Unreimbursed Charges And Credit Problems Meets Applicable Pleading Requirements

By itself, the factual allegation that consumers faced "unreimbursed charges" is sufficient to sustain the complaint. With more than 600,000 accounts compromised and more than $10 million in fraudulent charges, it is a fair inference that even small amounts of unreimbursed charges aggregate to substantial collective harm.

Wyndham asserts that, as a general matter, credit card issuers make a practice of reimbursing consumers for any fraudulent charges and that its customers therefore have suffered no harm. Br. at 48 & n.7, 50. In other words, Wyndham asserts that the FTC's facts do not show substantial harm to consumers because *other* alleged facts, outside the four corners of the complaint, show that there was no such harm. That, however, is not a failure of pleading, but a factual question on the merits. In ruling on a motion to dismiss, the Court does not "go beyond facts alleged in the Complaint." *In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1424–1425 (3d Cir. 1997). Thus, at this point in the case, the Court "must accept[] as true" the FTC's alleged facts, and it must "draw[] reasonable inferences in favor of the FTC, not [Wyndham]." *Opinion* 27-28 (JA 28-29) (citing *Iqbal*, 556 U.S. at 678, and *Phillips v. Cnty. of Allegheny*, 515 F.3d 224, 233-234 (3d Cir. 2008)).[19]

Wyndham's entire challenge to the sufficiency of the complaint fails for that reason alone. In any event, that challenge would fail even if it were appropriate to

[19] Wyndham also asserts that "[f]ederal law … generally caps consumer liability for credit or debit card fraud at $50." Br. 48. Even if the Court could take judicial notice of what federal law "generally" provides, $50 is not a de minimis loss even for an individual consumer. Particularly when aggregated, $50 per-consumer losses easily satisfy the statutory requirement of "substantial injury," 15 U.S.C. § 45(n), a standard that contains no minimum dollar threshold. *See American Financial*, 767 F.2d at 972 ("An injury may be sufficiently substantial … if it does a small harm to a large number of people[.]").

examine extrinsic facts at this stage. Merely because card issuers allegedly *promised* to give their customers refunds to cover all fraud losses does not mean that they actually *did* so. For example, some customers might not have detected the fraudulent charges; even if they detected the charges, they might not have undertaken the effort and expense of seeking a refund; and even if they asked, such refunds might not have been forthcoming.

That is why the Commission and the courts have long rejected the proposition that a "guarantee of … [a] refund prevents injury to the public" and immunizes perpetrators of unfair or deceptive practices from liability. *In re Michigan Bulb Co.*, 54 F.T.C. 1329, 1370 (1958) (citing *Capon Springs Mineral Water, Inc. v. FTC*, 107 F.2d 516, 519 (3d Cir. 1939)). "[A] money-back guaranty does not sanitize a fraud." *FTC v. Think Achievement Corp.*, 312 F.3d 259, 262 (7th Cir. 2002) (Posner, J.). Thus, a practice that causes consumers to incur unauthorized or fraudulent charges may violate Section 5 even if the perpetrator offers full refunds to dissatisfied consumers because "many consumers would not bother to seek" such a refund, especially if the amount is relatively small and the process of "obtaining a refund [is not] costless." *Id*. at 261 (citing *Montgomery Ward & Co. v. FTC*, 379 F.2d 666, 671 (7th Cir. 1967); *FTC v. Pantron I Corp.*, 33 F.3d 1088, 1103 (9th Cir. 1994); and *FTC v. SlimAmerica, Inc.*, 77 F. Supp. 2d 1263, 1273 (S.D. Fla. 1999)).

Wyndham asserts that to the (factually uncertain) extent consumers failed to take advantage of an offered reimbursement because they "neglected to review their statements and paid the fraudulent charges without questioning them," that is "a 'reasonably avoidable' injury" under Section 5(n). Br. 49. This argument, too, is unavailing. Wyndham does not argue that consumers could have avoided fraudulent bills in the first place. Consumers are powerless to prevent identity thieves from accessing and misusing their personal data when the business to which they entrust their information fails to secure it properly. Wyndham claims instead that even though its improper practices caused some consumers to pay fraudulent charges, Wyndham should be unaccountable because those consumers theoretically could have avoided paying the charges.

As the district court held, the question whether all consumers could avoid all charges is a "fact-dependent" one not suitable for disposition on a motion to dismiss. *Opinion* 32 (JA33). Moreover, Wyndham's argument sweeps too broadly. It asks that the Court allow Wyndham "to blame unsuspecting consumers for failing to detect and dispute unauthorized billing activity." *FTC v. Inc21.com Corp.*, 745 F.Supp.2d 975, 1004 (N.D. Cal. 2010), *aff'd*, 745 Fed.Appx. 106 (9th Cir. 2012). But "the burden should not be placed on defrauded customers to avoid charges that were never authorized to begin with." *Id*.

It is also immaterial that "the complaint fails to identify any [individual] consumer who suffered any financial injury." Br. 46 (emphasis omitted); *see also id.* 49-50. The complaint alleges that hundreds of thousands of credit card accounts were compromised and that at least *some* consumers suffered unreimbursed charges. Those facts are sufficient to state a plausible case of substantial consumer harm. Moreover, the FTC "need not identify specific victims" in statutory enforcement cases because, in many such cases, "the nature of the harm is so diffuse that the specific identities of the victims would be nearly impossible to ascertain." *FTC v. Bronson Partners LLC*, 654 F.3d 359, 373 (2d Cir. 2011). Relief is available even when it is "impossible or impracticable to locate and reimburse … individual consumers." *Pantron I Corp.*, 33 F.3d at 1103 n.34.

Finally, the complaint separately alleges that, in addition to unreimbursed charges, consumers unavoidably "lost access to funds or credit" as a result of fraudulent charges placed on their accounts. Cmplt. ¶40 (JA73). Given the number of accounts breached, that allegation independently constitutes a substantial injury and by itself suffices to sustain the complaint. Wyndham offers no contrary argument.

B. The Allegation That Customers Spent Time And Money Mitigating Harm Independently Meets Applicable Pleading Requirements

Quite apart from the allegations that the data breaches caused consumers unreimbursed charges, loss of access to funds, and credit problems, the complaint also alleges that customers spent "time and money resolving fraudulent charges and mitigating subsequent harm." Cmplt. ¶40 (JA73). That allegation, too, is independently sufficient to meet applicable pleading standards.

Because consumers entrusted their account data to Wyndham and could not protect it by themselves, they could not avoid the time and effort necessary to undo the damage of these data breaches and restore their credit, nor could they avoid the direct and opportunity costs of that wasted time. For example, they had to spend untold hours on the phone with their credit-card companies; find alternative sources of credit (if possible) while their accounts were on hold and before new cards were issued; and risk account suspensions with merchants who had used the voided cards for automatic renewals. Wyndham does not deny that the complaint alleges these and similar consumer harms, all of which resulted from Wyndham's negligence. Instead, Wyndham relies on *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), for the proposition that "efforts to redress … exposure" of credit card data do not state a claim of substantial injury as a matter of law. Br. 47. But *Reilly* is inapposite for two basic reasons.

First, after the hacker in *Reilly* breached the firewall of a payroll processor's computer system, it was "not known whether the hacker read, copied, or understood the data" to which it potentially gained access. *Reilly*, 664 F.3d at 40. There was thus "no evidence that the intrusion was intentional or malicious," and "no identifiable taking [of data] occurred; all that is known is that a firewall was penetrated." *Id*. at 44. On those facts, the Court held that a person whose information was stored in the computer system had suffered no injury sufficient to confer Article III standing. Rather, the claimed injury depended on "speculation" that the hacker actually acquired personal data, "intend[ed] to commit future criminal acts by misusing the information," and was "able to … mak[e] unauthorized transactions." *Id*. at 42. "Unless and until these conjectures come true," the Court held, plaintiff had "not suffered any injury." *Id*. Without "misuse of the information," there is "no harm." *Id*. In those circumstances, plaintiff's "alleged time and money expenditures" were speculative byproducts of the hypothetical harm. *Id*. at 46.

Wyndham misreads *Reilly* as holding categorically that consumer efforts to mitigate the effects of a data breach cannot constitute substantial injury. But *Reilly* addresses injury only *when there is no claim that data were stolen or misused*. Here, in contrast, the complaint alleges *actual* theft of data and *actual* misuse of that data: data were stolen, exported to Russia, and used to place more than $10

million of fraudulent charges on customer accounts. There is nothing speculative or hypothetical about the harmful use of the stolen data.

In cases of actual misuse, courts have held that the time, expense, and effort spent by consumers to mitigate injuries constitutes substantial injury under Section 5(n). In *Neovi*, which involved fraudulent checks, the Ninth Circuit found substantial injury on the ground that "obtaining reimbursement required a substantial investment of time, trouble, aggravation, and money. … Regardless of whether a bank eventually restored consumers' money, the consumer suffered unavoidable injuries that could not be fully mitigated." *Neovi*, 604 F.3d at 1158 (internal quotation marks omitted). Similarly, in a case involving the unlawful sale of telephone data, the Tenth Circuit held that "costs in changing telephone providers" were sufficient harm under Section 5(n). *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1194 (10th Cir. 2009).

Second, *Reilly* is inapplicable for the independent reason that it concerned the standing of private plaintiffs under Article III, not the ability of a federal agency to bring an action to enforce a consumer-protection statute. Congress has charged the Commission with enforcing the FTC Act and empowered it to bring suit to do so. 15 U.S.C. § 53(b). Whereas a private plaintiff must show that injury is "actual or imminent" and "affect[s] [him or her] in a personal and individual way," *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 & n.1 (1992), the FTC

need show only that Wyndham's practices "cause *or are likely to cause*" injury to any class of consumers. 15 U.S.C. § 45(n) (emphasis added); *see also SEC v. Rana Research, Inc.*, 8 F.3d 1358, 1363-1364 (9th Cir. 1993) (holding that under the securities antifraud laws, the government need not prove investor reliance or loss causation in enforcement actions). Here, whether or not an individual plaintiff could show particularized injury sufficient to satisfy Article III, the export of consumer credit card information to Russia is likely to cause injury simply because the information is in the hands of people who can use it—and have used it—to commit fraud.

CONCLUSION

The district court's decision should be affirmed.

Respectfully submitted,

/s/ Joel Marcus

JONATHAN E. NUECHTERLEIN
General Counsel

DAVID C. SHONKA
Principal Deputy General Counsel

JOEL MARCUS (D.C. BAR NO. 428680)
DAVID SIERADZKI
Attorneys

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
(202) 326-3350

Of Counsel:

KEVIN H. MORIARTY
JAMES A. TRILLING
KATHERINE E. MCCARRON
Attorneys
Bureau of Consumer Protection

November 5, 2014

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS

I. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because the brief contains 13,897 words.

II. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010, in 14-point Times New Roman.

November 5, 2015 /s/ Joel Marcus

CERTIFICATE OF IDENTICAL COMPLIANCE OF BRIEFS

I certify that the text of the electronically filed brief is identical to the text of the original copies that were sent on November 5, 2014, to the Clerk of the Court of the United States Court of Appeals for the Third Circuit.

November 5, 2014 /s/ Joel Marcus

CERTIFICATE OF PERFORMANCE OF VIRUS CHECK

I certify that on October 6, 2014, I performed a virus check on the electronically filed copy of this brief using Symantec Endpoint Protection version 12.1.4112.4156 (last updated Nov. 3, 2014). No virus was detected.

November 5, 2014 /s/ Joel Marcus

CERTIFICATE OF SERVICE

I certify that on November 5, 2014, I electronically filed the foregoing Brief for the Federal Trade Commission with the Clerk of the Court for the United States Court of Appeals for the Third Circuit by using the appellate CM/ECF system. All parties to this case will be served by the CM/ECF system.

November 5, 2014 /s/ Joel Marcus

STATUTORY APPENDIX

15 U.S.C. § 45

United States Code Annotated
Title 15. Commerce and Trade
Chapter 2. Federal Trade Commission; Promotion of Export Trade and Prevention of Unfair Methods of Competition
Subchapter I. Federal Trade Commission (Refs & Annos)

15 U.S.C.A. § 45

§ 45. Unfair methods of competition unlawful; prevention by Commission

Effective: December 22, 2006
Currentness

(a) Declaration of unlawfulness; power to prohibit unfair practices; inapplicability to foreign trade

(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.

(2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 57a(f)(3) of this title, Federal credit unions described in section 57a(f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of Title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended [7 U.S.C.A. § 181 et seq.], except as provided in section 406(b) of said Act [7 U.S.C.A. § 227(b)], from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

(3) This subsection shall not apply to unfair methods of competition involving commerce with foreign nations (other than import commerce) unless--

(A) such methods of competition have a direct, substantial, and reasonably foreseeable effect--

(i) on commerce which is not commerce with foreign nations, or on import commerce with foreign nations; or

(ii) on export commerce with foreign nations, of a person engaged in such commerce in the United States; and

(B) such effect gives rise to a claim under the provisions of this subsection, other than this paragraph.

If this subsection applies to such methods of competition only because of the operation of subparagraph (A)(ii), this subsection shall apply to such conduct only for injury to export business in the United States.

(4)(A) For purposes of subsection (a) of this section, the term “unfair or deceptive acts or practices” includes such acts or practices involving foreign commerce that--

(i) cause or are likely to cause reasonably foreseeable injury within the United States; or

(ii) involve material conduct occurring within the United States.

(B) All remedies available to the Commission with respect to unfair and deceptive acts or practices shall be available for acts and practices described in this paragraph, including restitution to domestic or foreign victims.

(b) Proceeding by Commission; modifying and setting aside orders

Whenever the Commission shall have reason to believe that any such person, partnership, or corporation has been or is using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce, and if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public, it shall issue and serve upon such person, partnership, or corporation a complaint stating its charges in that respect and containing a notice of a hearing upon a day and at a place therein fixed at least thirty days after the service of said complaint. The person, partnership, or corporation so complained of shall have the right to appear at the place and time so fixed and show cause why an order should not be entered by the Commission requiring such person, partnership, or corporation to cease and desist from the violation of the law so charged in said complaint. Any person, partnership, or corporation may make application, and upon good cause shown may be allowed by the Commission to intervene and appear in said proceeding by counsel or in person. The testimony in any such proceeding shall be reduced to writing and filed in the office of the Commission. If upon such hearing the Commission shall be of the opinion that the method of competition or the act or practice in question is prohibited by this subchapter, it shall make a report in writing in which it shall state its findings as to the facts and shall issue and cause to be served on such person, partnership, or corporation an order requiring such person, partnership, or corporation to cease and desist from using such method of competition or such act or practice. Until the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time, or, if a petition for review has been filed within such time then until the record in the proceeding has been filed in a court of appeals of the United States, as hereinafter provided, the Commission may at any time, upon such notice and in such manner as it shall deem proper, modify or set aside, in whole or in part, any report or any order made or issued by it under this section. After the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time, the Commission may at any time, after notice and opportunity for hearing, reopen and alter, modify, or set aside, in whole or in part, any report or order made or issued by it under this section, whenever in the opinion of the Commission conditions of fact or of law have so changed as to require such action or if the public interest shall so require, except that (1) the said person, partnership, or corporation may, within sixty days after service upon him or it of said report or order entered after such a reopening, obtain a review thereof in the appropriate court of appeals of the United States, in the manner provided in subsection (c) of this section; and (2) in the case of an order, the Commission shall reopen any such order to consider whether such order (including any affirmative relief provision contained in such order) should be altered, modified, or set aside, in whole or in part, if the person, partnership, or corporation involved files a request with the Commission which makes a satisfactory showing that changed conditions of law or fact require such order to be altered, modified, or set aside, in whole or in part. The Commission shall determine whether to alter, modify, or set aside any order of the Commission in response to a request made by a person, partnership, or corporation under paragraph [1] (2) not later than 120 days after the date of the filing of such request.

(c) Review of order; rehearing

Any person, partnership, or corporation required by an order of the Commission to cease and desist from using any method of competition or act or practice may obtain a review of such order in the court of appeals of the United States, within any circuit where the method of competition or the act or practice in question was used or where such person, partnership, or corporation resides or carries on business, by filing in the court, within sixty days from the date of the service of such order, a written

petition praying that the order of the Commission be set aside. A copy of such petition shall be forthwith transmitted by the clerk of the court to the Commission, and thereupon the Commission shall file in the court the record in the proceeding, as provided in section 2112 of Title 28. Upon such filing of the petition the court shall have jurisdiction of the proceeding and of the question determined therein concurrently with the Commission until the filing of the record and shall have power to make and enter a decree affirming, modifying, or setting aside the order of the Commission, and enforcing the same to the extent that such order is affirmed and to issue such writs as are ancillary to its jurisdiction or are necessary in its judgement to prevent injury to the public or to competitors pendente lite. The findings of the Commission as to the facts, if supported by evidence, shall be conclusive. To the extent that the order of the Commission is affirmed, the court shall thereupon issue its own order commanding obedience to the terms of such order of the Commission. If either party shall apply to the court for leave to adduce additional evidence, and shall show to the satisfaction of the court that such additional evidence is material and that there were reasonable grounds for the failure to adduce such evidence in the proceeding before the Commission, the court may order such additional evidence to be taken before the Commission and to be adduced upon the hearing in such manner and upon such terms and conditions as to the court may seem proper. The Commission may modify its findings as to the facts, or make new findings, by reason of the additional evidence so taken, and it shall file such modified or new findings, which, if supported by evidence, shall be conclusive, and its recommendation, if any, for the modification or setting aside of its original order, with the return of such additional evidence. The judgment and decree of the court shall be final, except that the same shall be subject to review by the Supreme Court upon certiorari, as provided in section 1254 of Title 28.

(d) Jurisdiction of court

Upon the filing of the record with it the jurisdiction of the court of appeals of the United States to affirm, enforce, modify, or set aside orders of the Commission shall be exclusive.

(e) Exemption from liability

No order of the Commission or judgement of court to enforce the same shall in anywise relieve or absolve any person, partnership, or corporation from any liability under the Antitrust Acts.

(f) Service of complaints, orders and other processes; return

Complaints, orders, and other processes of the Commission under this section may be served by anyone duly authorized by the Commission, either (a) by delivering a copy thereof to the person to be served, or to a member of the partnership to be served, or the president, secretary, or other executive officer or a director of the corporation to be served; or (b) by leaving a copy thereof at the residence or the principal office or place of business of such person, partnership, or corporation; or (c) by mailing a copy thereof by registered mail or by certified mail addressed to such person, partnership, or corporation at his or its residence or principal office or place of business. The verified return by the person so serving said complaint, order, or other process setting forth the manner of said service shall be proof of the same, and the return post office receipt for said complaint, order, or other process mailed by registered mail or by certified mail as aforesaid shall be proof of the service of the same.

(g) Finality of order

An order of the Commission to cease and desist shall become final--

(1) Upon the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time; but the Commission may thereafter modify or set aside its order to the extent provided in the last sentence of subsection (b).

(2) Except as to any order provision subject to paragraph (4), upon the sixtieth day after such order is served, if a petition for review has been duly filed; except that any such order may be stayed, in whole or in part and subject to such conditions as may be appropriate, by--

(A) the Commission;

(B) an appropriate court of appeals of the United States, if (i) a petition for review of such order is pending in such court, and (ii) an application for such a stay was previously submitted to the Commission and the Commission, within the 30-day period beginning on the date the application was received by the Commission, either denied the application or did not grant or deny the application; or

(C) the Supreme Court, if an applicable petition for certiorari is pending.

(3) For purposes of subsection (m)(1)(B) of this section and of section 57b(a)(2) of this title, if a petition for review of the order of the Commission has been filed--

(A) upon the expiration of the time allowed for filing a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals and no petition for certiorari has been duly filed;

(B) upon the denial of a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals; or

(C) upon the expiration of 30 days from the date of issuance of a mandate of the Supreme Court directing that the order of the Commission be affirmed or the petition for review be dismissed.

(4) In the case of an order provision requiring a person, partnership, or corporation to divest itself of stock, other share capital, or assets, if a petition for review of such order of the Commission has been filed--

(A) upon the expiration of the time allowed for filing a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals and no petition for certiorari has been duly filed;

(B) upon the denial of a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals; or

(C) upon the expiration of 30 days from the date of issuance of a mandate of the Supreme Court directing that the order of the Commission be affirmed or the petition for review be dismissed.

(h) Modification or setting aside of order by Supreme Court

If the Supreme Court directs that the order of the Commission be modified or set aside, the order of the Commission rendered in accordance with the mandate of the Supreme Court shall become final upon the expiration of thirty days from the time it was rendered, unless within such thirty days either party has instituted proceedings to have such order corrected to accord with the mandate, in which event the order of the Commission shall become final when so corrected.

(i) Modification or setting aside of order by Court of Appeals

If the order of the Commission is modified or set aside by the court of appeals, and if (1) the time allowed for filing a petition for certiorari has expired and no such petition has been duly filed, or (2) the petition for certiorari has been denied, or (3) the decision of the court has been affirmed by the Supreme Court, then the order of the Commission rendered in accordance with the mandate of the court of appeals shall become final on the expiration of thirty days from the time such order of the Commission was rendered, unless within such thirty days either party has instituted proceedings to have such order corrected so that it will accord with the mandate, in which event the order of the Commission shall become final when so corrected.

(j) Rehearing upon order or remand

If the Supreme Court orders a rehearing; or if the case is remanded by the court of appeals to the Commission for a rehearing, and if (1) the time allowed for filing a petition for certiorari has expired, and no such petition has been duly filed, or (2) the petition for certiorari has been denied, or (3) the decision of the court has been affirmed by the Supreme Court, then the order of the Commission rendered upon such rehearing shall become final in the same manner as though no prior order of the Commission had been rendered.

(k) “Mandate” defined

As used in this section the term “mandate”, in case a mandate has been recalled prior to the expiration of thirty days from the date of issuance thereof, means the final mandate.

(l) Penalty for violation of order; injunctions and other appropriate equitable relief

Any person, partnership, or corporation who violates an order of the Commission after it has become final, and while such order is in effect, shall forfeit and pay to the United States a civil penalty of not more than $10,000 for each violation, which shall accrue to the United States and may be recovered in a civil action brought by the Attorney General of the United States. Each separate violation of such an order shall be a separate offense, except that in a case of a violation through continuing failure to obey or neglect to obey a final order of the Commission, each day of continuance of such failure or neglect shall be deemed a separate offense. In such actions, the United States district courts are empowered to grant mandatory injunctions and such other and further equitable relief as they deem appropriate in the enforcement of such final orders of the Commission.

(m) Civil actions for recovery of penalties for knowing violations of rules and cease and desist orders respecting unfair or deceptive acts or practices; jurisdiction; maximum amount of penalties; continuing violations; de novo determinations; compromise or settlement procedure

(1)(A) The Commission may commence a civil action to recover a civil penalty in a district court of the United States against any person, partnership, or corporation which violates any rule under this chapter respecting unfair or deceptive acts or practices (other than an interpretive rule or a rule violation of which the Commission has provided is not an unfair or deceptive act or practice in violation of subsection (a)(1) of this section) with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule. In such action, such person, partnership, or corporation shall be liable for a civil penalty of not more than $10,000 for each violation.

(B) If the Commission determines in a proceeding under subsection (b) of this section that any act or practice is unfair or deceptive, and issues a final cease and desist order, other than a consent order, with respect to such act or practice, then the Commission may commence a civil action to obtain a civil penalty in a district court of the United States against any person, partnership, or corporation which engages in such act or practice--

(1) after such cease and desist order becomes final (whether or not such person, partnership, or corporation was subject to such cease and desist order), and

(2) with actual knowledge that such act or practice is unfair or deceptive and is unlawful under subsection (a)(1) of this section.

In such action, such person, partnership, or corporation shall be liable for a civil penalty of not more than $10,000 for each violation.

(C) In the case of a violation through continuing failure to comply with a rule or with subsection (a)(1) of this section, each day of continuance of such failure shall be treated as a separate violation, for purposes of subparagraphs (A) and (B). In determining the amount of such a civil penalty, the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require.

(2) If the cease and desist order establishing that the act or practice is unfair or deceptive was not issued against the defendant in a civil penalty action under paragraph (1)(B) the issues of fact in such action against such defendant shall be tried de novo. Upon request of any party to such an action against such defendant, the court shall also review the determination of law made by the Commission in the proceeding under subsection (b) of this section that the act or practice which was the subject of such proceeding constituted an unfair or deceptive act or practice in violation of subsection (a) of this section.

(3) The Commission may compromise or settle any action for a civil penalty if such compromise or settlement is accompanied by a public statement of its reasons and is approved by the court.

(n) Standard of proof; public policy consideration

The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless 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 to competition. 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.

CREDIT(S)

(Sept. 26, 1914, c. 311, § 5, 38 Stat. 719; Mar. 21, 1938, c. 49, § 3, 52 Stat. 111; June 23, 1938, c. 601, Title XI, § 1107(f), 52 Stat. 1028; June 25, 1948, c. 646, § 32(a), 62 Stat. 991; May 24, 1949, c. 139, § 127, 63 Stat. 107; Mar. 16, 1950, c. 61, § 4(c), 64 Stat. 21; July 14, 1952, c. 745, § 2, 66 Stat. 632; Aug. 23, 1958, Pub.L. 85-726, Title XIV, §§ 1401(b), 1411, 72 Stat. 806, 809; Aug. 28, 1958, Pub.L. 85-791, § 3, 72 Stat. 942; Sept. 2, 1958, Pub.L. 85-909, § 3, 72 Stat. 1750; June 11, 1960, Pub.L. 86-507, § 1(13), 74 Stat. 200; Nov. 16, 1973, Pub.L. 93-153, Title IV, § 408(c), (d), 87 Stat. 591, 592; Jan. 4, 1975, Pub.L. 93-637, Title II, §§ 201(a), 204(b), 205(a), 88 Stat. 2193, 2200; Dec. 12, 1975, Pub.L. 94-145, § 3, 89 Stat. 801; July 23, 1979, Pub.L. 96-37, § 1(a), 93 Stat. 95; May 28, 1980, Pub.L. 96-252, § 2, 94 Stat. 374; Oct. 8, 1982, Pub.L. 97-290, Title IV, § 403, 96 Stat. 1246; Nov. 8, 1984, Pub.L. 98-620, Title IV, § 402(12), 98 Stat. 3358; Aug. 10, 1987, Pub.L. 100-86, Title VII, § 715(a)(1), 101 Stat. 655; Aug. 26, 1994, Pub.L. 103-312, §§ 4, 6, 9, 108 Stat. 1691, 1692, 1695; Dec. 22, 2006, Pub.L. 109-455, § 3, 120 Stat. 3372.)

TERMINATION OF AMENDMENTS

<For repeal of Pub.L. 109-455 and the amendments made by Pub.L. 109-455, effective September 30, 2020, by section 13 of Pub.L. 109-455, as amended, see Sunset Provisions note set out under this section and 15 U.S.C.A. § 44. >

Notes of Decisions (2277)

Footnotes

1 So in original. Probably should be “clause”.

15 U.S.C.A. § 45, 15 USCA § 45

Current through P.L. 113-163 approved 8-8-14

End of Document

ATTACHMENT 1

2007 BUSINESS GUIDE

Protecting PERSONAL INFORMATION

A Guide for Business

FEDERAL TRADE COMMISSION

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW
Washington, DC 20580
1–877–FTC–HELP (1–877–382–4357)

ftc.gov

PROTECTING PERSONAL INFORMATION

A Guide for Business

Most companies keep sensitive personal information in their files—names, Social Security numbers, credit card, or other account data—that identifies customers or employees.

This information often is necessary to fill orders, meet payroll, or perform other necessary business functions. However, if sensitive data falls into the wrong hands, it can lead to fraud, identity theft, or similar harms. Given the cost of a security breach—losing your customers' trust and perhaps even defending yourself against a lawsuit—safeguarding personal information is just plain good business.

A sound data security plan is built on **5 key principles:**

1. **Take stock.** Know what personal information you have in your files and on your computers.

2. **Scale down.** Keep only what you need for your business.

3. **Lock it.** Protect the information that you keep.

4. **Pitch it.** Properly dispose of what you no longer need.

5. **Plan ahead.** Create a plan to respond to security incidents.

Use the checklists on the following pages to see how your company's practices measure up—and where changes are necessary.

1. TAKE STOCK. Know what personal information you have in your files and on your computers.

Effective data security starts with assessing what information you have and identifying who has access to it. Understanding how personal information moves into, through, and out of your business and who has—or could have—access to it is essential to assessing security vulnerabilities. You can determine the best ways to secure the information only after you've traced how it flows.

- Inventory all computers, laptops, flash drives, disks, home computers, and other equipment to find out where your company stores sensitive data. Also inventory the information you have by type and location. Your file cabinets and computer systems are a start, but remember: your business receives personal information in a number of ways—through websites, from contractors, from call centers, and the like. What about information saved on laptops, employees' home computers, flash drives, and cell phones? No inventory is complete until you check everywhere sensitive data might be stored.
- Track personal information through your business by talking with your sales department, information technology staff, human resources office, accounting personnel, and outside service providers. Get a complete picture of:

- ***Who sends sensitive personal information to your business.*** Do you get it from customers? Credit card companies? Banks or other financial institutions? Credit bureaus? Other businesses?
- ***How your business receives personal information.*** Does it come to your business through a website? By email? Through the mail? Is it transmitted through cash registers in stores?
- ***What kind of information you collect at each entry point.*** Do you get credit card information online? Does your accounting department keep information about customers' checking accounts?
- ***Where you keep the information you collect at each entry point.*** Is it in a central computer database? On individual laptops? On disks or tapes? In file cabinets? In branch offices? Do employees have files at home?
- ***Who has—or could have—access to the information.*** Which of your employees has permission to access the information? Could anyone else get a hold of it? What about vendors who supply and update software you use to process credit card transactions? Contractors operating your call center?

SECURITY CHECK

Question:

Are there laws that require my company to keep sensitive data secure?

Answer:

Yes. While you're taking stock of the data in your files, take stock of the law, too. Statutes like the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Federal Trade Commission Act may require you to provide reasonable security for sensitive information.

To find out more, visit ***www.ftc.gov/privacy***.

- Different types of information present varying risks. Pay particular attention to how you keep personally identifying information: Social Security numbers, credit card or financial information, and other sensitive data. That's what thieves use most often to commit fraud or identity theft.

2. SCALE DOWN. Keep only what you need for your business.

If you don't have a legitimate business need for sensitive personally identifying information, don't keep it. In fact, don't even collect it. If you have a legitimate business need for the information, keep it only as long as it's necessary.

- Use Social Security numbers only for required and lawful purposes—like reporting employee taxes. Don't use Social Security numbers unnecessarily—for example, as an employee or customer identification number, or because you've always done it.

SECURITY CHECK

Question:

We like to have accurate information about our customers, so we usually create a permanent file about all aspects of their transactions, including the information we collected from the magnetic stripe on their credit cards. Could this practice put their information at risk?

Answer:

Yes. Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not in your system, it can't be stolen by hackers. It's as simple as that.

- Don't keep customer credit card information unless you have a business need for it. For example, don't retain the account number and expiration date unless you have an essential business need to do so. Keeping this information—or keeping it longer than necessary—raises the risk that the information could be used to commit fraud or identity theft.
- Check the default settings on your software that reads customers' credit card numbers and processes the transactions. Sometimes it's preset to keep information permanently. Change the default setting to make sure you're not inadvertently keeping information you don't need.
- If you must keep information for business reasons or to comply with the law, develop a written records retention policy to identify what information must be kept, how to secure it, how long to keep it, and how to dispose of it securely when you no longer need it.

SCALE DOWN.

2

3. LOCK IT. Protect the information that you keep.

What's the best way to protect the sensitive personally identifying information you need to keep? It depends on the kind of information and how it's stored. The most effective data security plans deal with four key elements: physical security, electronic security, employee training, and the security practices of contractors and service providers.

PHYSICAL SECURITY

Many data compromises happen the old-fashioned way—through lost or stolen paper documents. Often, the best defense is a locked door or an alert employee.

- Store paper documents or files, as well as CDs, floppy disks, zip drives, tapes, and backups containing personally identifiable information in a locked room or in a locked file cabinet. Limit access to employees with a legitimate business need. Control who has a key, and the number of keys.

- Require that files containing personally identifiable information be kept in locked file cabinets except when an employee is working on the file. Remind employees not to leave sensitive papers out on their desks when they are away from their workstations.
- Require employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.
- Implement appropriate access controls for your building. Tell employees what to do and whom to call if they see an unfamiliar person on the premises.
- If you maintain offsite storage facilities, limit employee access to those with a legitimate business need. Know if and when someone accesses the storage site.
- If you ship sensitive information using outside carriers or contractors, encrypt the information and keep an inventory of the information being shipped. Also use an overnight shipping service that will allow you to track the delivery of your information.

ELECTRONIC SECURITY

Computer security isn't just the realm of your IT staff. Make it your business to understand the vulnerabilities of your computer system, and follow the advice of experts in the field.

General Network Security

- Identify the computers or servers where sensitive personal information is stored.
- Identify all connections to the computers where you store sensitive information. These may include the Internet, electronic cash registers, computers at your branch offices, computers used by service providers to support your network, and wireless devices like inventory scanners or cell phones.

- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks. Depending on your circumstances, appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit.
- Don't store sensitive consumer data on any computer with an Internet connection unless it's essential for conducting your business.
- Encrypt sensitive information that you send to third parties over public networks (like the Internet), and consider encrypting sensitive information that is stored on your computer network or on disks or portable storage devices used by your employees. Consider also encrypting email transmissions within your business if they contain personally identifying information.
- Regularly run up-to-date anti-virus and anti-spyware programs on individual computers and on servers on your network.
- Check expert websites (such as ***www.sans.org***) and your software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches to correct problems.
- Scan computers on your network to identify and profile the operating system and open network services. If you find services that you don't need, disable them to prevent hacks or other potential security problems. For example, if email service or an Internet connection is not necessary on a certain computer, consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
- When you receive or transmit credit card information or other sensitive financial data, use Secure Sockets Layer (SSL) or another secure connection that protects the information in transit.

SECURITY CHECK

Question:

We encrypt financial data customers submit on our website. But once we receive it, we decrypt it and email it over the Internet to our branch offices in regular text. Is there a safer practice?

Answer:

Yes. Regular email is not a secure method for sending sensitive data. The better practice is to encrypt any transmission that contains information that could be used by fraudsters or ID thieves.

- Pay particular attention to the security of your web applications—the software used to give information to visitors to your website and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks. In one variation called an "injection attack," a hacker inserts malicious commands into what looks like a legitimate request for information. Once in your system, hackers transfer sensitive information from your network to their computers. Relatively simple defenses against these attacks are available from a variety of sources.

Password Management

- Control access to sensitive information by requiring that employees use "strong" passwords. Tech security experts say the longer the password, the better. Because simple passwords—like common dictionary words—can be guessed easily, insist that employees choose passwords with a mix of letters, numbers, and characters. Require an employee's user name and password to be different, and require frequent changes in passwords.
- Explain to employees why it's against company policy to share their passwords or post them near their workstations.
- Use password-activated screen savers to lock employee computers after a period of inactivity.
- Lock out users who don't enter the correct password within a designated number of log-on attempts.

SECURITY CHECK

Question:

Our account staff needs access to our database of customer financial information. To make it easier to remember, we just use our company name as the password. Could that create a security problem?

Answer:

Yes. Hackers will first try words like "password," your company name, the software's default password, and other easy-to-guess choices. They'll also use programs that run through common English words and dates. To make it harder for them to crack your system, select strong passwords—the longer, the better—that use a combination of letters, symbols, and numbers. And change passwords often.

- Warn employees about possible calls from identity thieves attempting to deceive them into giving out their passwords by impersonating members of your IT staff. Let employees know that calls like this are always fraudulent, and that no one should be asking them to reveal their passwords.
- When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
- Caution employees against transmitting sensitive personally identifying data—Social Security numbers, passwords, account information—via email. Unencrypted email is not a secure way to transmit any information.

Laptop Security

- Restrict the use of laptops to those employees who need them to perform their jobs.
- Assess whether sensitive information really needs to be stored on a laptop. If not, delete it with a "wiping" program that overwrites data on the laptop. Deleting files using standard keyboard commands isn't sufficient because data may remain on the laptop's hard drive. Wiping programs are available at most office supply stores.
- Require employees to store laptops in a secure place. Even when laptops are in use, consider using cords and locks to secure laptops to employees' desks.

- Consider allowing laptop users only to access sensitive information, but not to store the information on their laptops. Under this approach, the information is stored on a secure central computer and the laptops function as terminals that display information from the central computer, but do not store it. The information could be further protected by requiring the use of a token, "smart card," thumb print, or other biometric—as well as a password—to access the central computer.
- If a laptop contains sensitive data, encrypt it and configure it so users can't download any software or change the security settings without approval from your IT specialists. Consider adding an "auto-destroy" function so that data on a computer that is reported stolen will be destroyed when the thief uses it to try to get on the Internet.
- Train employees to be mindful of security when they're on the road. They should never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage unless directed to by airport security. If someone must leave a laptop in a car, it should be locked in a trunk. Everyone who goes through airport security should keep an eye on their laptop as it goes on the belt.

Firewalls

- Use a firewall to protect your computer from hacker attacks while it is connected to the Internet. A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files.
- Determine whether you should install a "border" firewall where your network connects to the Internet. A border firewall separates your network from the Internet and may prevent an attacker from gaining access to a computer on the network where you store sensitive information. Set "access controls"—settings that determine who gets through the firewall and what they will be allowed to see—to allow only trusted employees with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, review them periodically.
- If some computers on your network store sensitive information while others do not, consider using additional firewalls to protect the computers with sensitive information.

Wireless and Remote Access

- Determine if you use wireless devices like inventory scanners or cell phones to connect to your computer network or to transmit sensitive information.
- If you do, consider limiting who can use a wireless connection to access your computer network. You can make it harder for an intruder to access the network by limiting the wireless devices that can connect to your network.
- Better still, consider encryption to make it more difficult for an intruder to read the content. Encrypting transmissions from wireless devices to your computer network may prevent an intruder from gaining access through a process called "spoofing"—impersonating one of your computers to get access to your network.
- Consider using encryption if you allow remote access to your computer network by employees or by service providers, such as companies that troubleshoot and update software you use to process credit card purchases.

Detecting Breaches

- To detect network breaches when they occur, consider using an intrusion detection system. To be effective, it must be updated frequently to address new types of hacking.
- Maintain central log files of security-related information to monitor activity on your network so that you can spot and respond to attacks. If there is an attack on your network, the log will provide information that can identify the computers that have been compromised.

- Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.
- Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from your system to an unknown user. If large amounts of information are being transmitted from your network, investigate to make sure the transmission is authorized.
- Have in place and implement a breach response plan. See pages 22–23 for more information.

EMPLOYEE TRAINING

Your data security plan may look great on paper, but it's only as strong as the employees who implement it. Take time to explain the rules to your staff, and train them to spot security vulnerabilities. Periodic training emphasizes the importance you place on meaningful data security practices. A well-trained workforce is the best defense against identity theft and data breaches.

- Check references or do background checks before hiring employees who will have access to sensitive data.
- Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling sensitive data. Make sure they understand that abiding by your company's data security plan is an essential part of their duties. Regularly remind employees of your company's policy—and any legal requirement—to keep customer information secure and confidential.
- Know which employees have access to consumers' sensitive personally identifying information. Pay particular attention to data like Social Security numbers and account numbers. Limit access to personal information to employees with a "need to know."
- Have a procedure in place for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information. Terminate their passwords, and collect keys and identification cards as part of the check-out routine.

SECURITY CHECK

Question:

I'm not really a "tech" type. Are there steps our computer people can take to protect our system from common hack attacks?

Answer:

Yes. There are relatively simple fixes to protect your computers from some of the most common vulnerabilities. For example, a threat called an "SQL injection attack" can give fraudsters access to sensitive data on your system, but can be thwarted with a simple change to your computer. Bookmark the websites of groups like the Open Web Application Security Project, ***www.owasp.org***, or SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities, ***www.sans.org/top20***, for up-to-date information on the latest threats—and fixes. And check with your software vendors for patches that address new vulnerabilities.

- Create a "culture of security" by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. Make sure training includes employees at satellite offices, temporary help, and seasonal workers. If employees don't attend, consider blocking their access to the network.
- Train employees to recognize security threats. Tell them how to report suspicious activity and publicly reward employees who alert you to vulnerabilities.

- Tell employees about your company policies regarding keeping information secure and confidential. Post reminders in areas where sensitive information is used or stored, as well as where employees congregate. Make sure your policies cover employees who telecommute or access sensitive data from home or an offsite location.
- Warn employees about phone phishing. Train them to be suspicious of unknown callers claiming to need account numbers to process an order or asking for customer or employee contact information. Make it office policy to double-check by contacting the company using a phone number you know is genuine.
- Require employees to notify you immediately if there is a potential security breach, such as a lost or stolen laptop.
- Impose disciplinary measures for security policy violations.
- For computer security tips, tutorials, and quizzes for everyone on your staff, visit ***www.OnGuardOnline.gov***.

SECURITY PRACTICES OF CONTRACTORS AND SERVICE PROVIDERS

Your company's security practices depend on the people who implement them, including contractors and service providers.

- Before you outsource any of your business functions—payroll, web hosting, customer call center operations, data processing, or the like—investigate the company's data security practices and compare their standards to yours. If possible, visit their facilities.
- Address security issues for the type of data your service providers handle in your contract with them.
- Insist that your service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of your data.

4. PITCH IT. Properly dispose of what you no longer need.

What looks like a sack of trash to you can be a gold mine for an identity thief. Leaving credit card receipts or papers or CDs with personally identifying information in a dumpster facilitates fraud and exposes consumers to the risk of identity theft. By properly disposing of sensitive information, you ensure that it cannot be read or reconstructed.

- Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to—or use of—personally identifying information. Reasonable measures for your operation are based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.

SECURITY CHECK

Question:

My company collects credit applications from customers. The form requires them to give us lots of financial information. Once we're finished with the applications, we're careful to throw them away. Is that sufficient?

Answer:

No. Have a policy in place to ensure that sensitive paperwork is unreadable before you throw it away. Burn it, shred it, or pulverize it to make sure identity thieves can't steal it from your trash.

- Effectively dispose of paper records by shredding, burning, or pulverizing them before discarding. Make shredders available throughout the workplace, including next to the photocopier.
- When disposing of old computers and portable storage devices, use wipe utility programs. They're inexpensive and can provide better results by overwriting the entire hard drive so that the files are no longer recoverable. Deleting files using the keyboard or mouse commands usually isn't sufficient because the files may continue to exist on the computer's hard drive and could be retrieved easily.
- Make sure employees who work from home follow the same procedures for disposing of sensitive documents and old computers and portable storage devices.
- If you use consumer credit reports for a business purpose, you may be subject to the FTC's Disposal Rule. For more information, see *Disposing of Consumer Report Information? New Rule Tells How* at ***www.ftc.gov/privacy*** (click on Credit Reporting, Business Guidance).

5. PLAN AHEAD. Create a plan for responding to security incidents.

Taking steps to protect data in your possession can go a long way toward preventing a security breach. Nevertheless, breaches can happen. Here's how you can reduce the impact on your business, your employees, and your customers:

- Have a plan in place to respond to security incidents. Designate a senior member of your staff to coordinate and implement the response plan.
- If a computer is compromised, disconnect it immediately from the Internet.

SECURITY CHECK

Question:

I own a small business. Aren't these precautions going to cost me a mint to implement?

Answer:

No. There's no one-size-fits-all approach to data security, and what's right for you depends on the nature of your business and the kind of information you collect from your customers. Some of the most effective security measures—using strong passwords, locking up sensitive paperwork, training your staff, etc.—will cost you next to nothing and you'll find free or low-cost security tools at non-profit websites dedicated to data security. Furthermore, it's cheaper in the long run to invest in better data security than to lose the goodwill of your customers, defend yourself in legal actions, and face other possible consequences of a data breach.

- Investigate security incidents immediately and take steps to close off existing vulnerabilities or threats to personal information.
- Consider whom to notify in the event of an incident, both inside and outside your organization. You may need to notify consumers, law enforcement, customers, credit bureaus, and other businesses that may be affected by the breach. In addition, many states and the federal bank regulatory agencies have laws or guidelines addressing data breaches. Consult your attorney.

ADDITIONAL RESOURCES

These websites and publications have more information on securing sensitive data:

- National Institute of Standards and Technology (NIST)'s Computer Security Resource Center
  www.csrc.nist.gov
- NIST's Risk Management Guide for Information Technology Systems
  www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Department of Homeland Security's National Strategy to Secure Cyberspace
  www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf
- SANS (SysAdmin, Audit, Network, Security) Institute's Twenty Most Critical Internet Security Vulnerabilities
  www.sans.org/top20
- United States Computer Emergency Readiness Team (US-CERT)
  www.us-cert.gov
- Carnegie Mellon Software Engineering Institute's CERT Coordination Center
  www.cert.org/other_sources
- Center for Internet Security (CIS)
  www.cisecurity.org
- The Open Web Application Security Project
  www.owasp.org
- Institute for Security Technology Studies
  www.ists.dartmouth.edu
- OnGuard Online
  www.OnGuardOnline.gov

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free 1–877–FTC-HELP (1–877–382–4357); TTY: 1–866–653–4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Opportunity to Comment

The Small Business and Agriculture Regulatory Enforcement Ombudsman and 10 Regional Fairness Boards collect comments from small business about federal enforcement actions. Each year, the Ombudsman evaluates enforcement activities and rates each agency's responsiveness to small business. To comment on FTC actions, call 1–888–734–3247.

FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, NW
Washington, DC 20580
1–877–FTC–HELP (1–877–382–4357)

ftc.gov

ATTACHMENT 2

LABMD ORDER

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	
	)	**DOCKET NO. 9357**
LabMD, Inc.,	)	
a corporation.	)	**PUBLIC**
	)	

ORDER DENYING RESPONDENT LABMD'S MOTION TO DISMISS

By Commissioner Joshua D. Wright, for a unanimous Commission:[1]

This case presents fundamental questions about the authority of the Federal Trade Commission ("FTC" or "the Commission") to protect consumers from harmful business practices in the increasingly important field of data security. In our interconnected and data-driven economy, businesses are collecting more personal information about their customers and other individuals than ever before. Companies store this information in digital form on their computer systems and networks, and often transact business by transmitting and receiving such data over the Internet and other public networks. This creates a fertile environment for hackers and others to exploit computer system vulnerabilities, covertly obtain access to consumers' financial, medical, and other sensitive information, and potentially misuse it in ways that can inflict serious harms on consumers. Businesses that store, transmit, and use consumer information can, however, implement safeguards to reduce the likelihood of data breaches and help prevent sensitive consumer data from falling into the wrong hands.

Respondent LabMD, Inc. ("LabMD") has moved to dismiss the Complaint in this adjudicatory proceeding, arguing that the Commission has no authority to address private companies' data security practices as "unfair . . . acts or practices" under Section 5(a)(1) of the Federal Trade Commission Act ("FTC Act" or "the Act"), 15 U.S.C. § 45(a)(1). This view, if accepted, would greatly restrict the Commission's ability to protect consumers from unwanted privacy intrusions, fraudulent misuse of their personal information, or even identity theft that may result from businesses' failure to establish and maintain reasonable and appropriate data security measures. The Commission would be unable to hold a business accountable for its conduct, even if its data security program is so inadequate that it "causes or is likely to cause

[1] Commissioner Brill did not take part in the consideration or decision herein.

substantial injury to consumers [that] is not reasonably avoidable by consumers themselves and [such injury is] not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n).

LabMD's Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings ("Motion to Dismiss" or "Motion"), filed November 12, 2013, calls on the Commission to decide whether the FTC Act's prohibition of "unfair . . . acts or practices" applies to a company's failure to implement reasonable and appropriate data security measures. We conclude that it does. We also reject LabMD's contention that, by enacting the Health Insurance Portability and Accountability Act ("HIPAA") and other statutes touching on data security, Congress has implicitly stripped the Commission of authority to enforce Section 5 of the FTC Act in the field of data security, despite the absence of any express statutory language to that effect. Nor can we accept the premise underlying LabMD's "due process" arguments – that, in effect, companies are free to violate the FTC Act's prohibition of "unfair . . . acts or practices" without fear of enforcement actions by the Commission, unless the Commission has first adopted regulations. Accordingly, we deny LabMD's Motion to Dismiss.

PROCEDURAL BACKGROUND

On August 28, 2013, the Commission issued an administrative complaint ("Complaint") against LabMD, a Georgia-based company in the business of conducting clinical laboratory tests on specimen samples from consumers and reporting test results to consumers' health care providers. The Complaint alleges that LabMD engaged in "practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks," *see* Complaint, ¶ 10; that these practices caused harm to consumers, including exposure to identity theft and disclosure of sensitive, private medical information, *id.*, ¶¶ 12, 17-21; and, consequently, that LabMD engaged in "unfair . . . acts or practices" in violation of the FTC Act. *Id*., ¶¶ 22-23. LabMD submitted its Answer and Affirmative Defenses to the Administrative Complaint ("Answer") on September 17, 2013.

LabMD filed its Motion to Dismiss on November 12, 2013.[2] On November 22, 2013, Complaint Counsel filed its Response in Opposition to Respondent's Motion to Dismiss Complaint with Prejudice ("CC Opp."). LabMD filed its Reply to Complaint Counsel's Response in Opposition to Respondent's Motion to Dismiss ("Reply") on December 2, 2013. Factual discovery is now underway and is scheduled to close on March 5, 2014. The evidentiary hearing before the Administrative Law Judge is scheduled to begin on May 20, 2014.

[2] The Commission issued an Order on December 13, 2013, denying both LabMD's request for a stay of the administrative proceedings pending resolution of its Motion to Dismiss (*see* Motion at 29-30) and a separate Motion for Stay Pending Judicial Review that LabMD filed on November 26, 2013.

STANDARD OF REVIEW

We review LabMD's Motion to Dismiss using the standards a reviewing court would apply in assessing a motion to dismiss for failure to state a claim.[3] *See* Fed. R. Civ. P. 12(b)(6); *see also* Motion at 8; CC Opp. at 3; *S.C. State Bd. of Dentistry*, 138 F.T.C. 230, 232-33 (2004); *Union Oil Co.*, 138 F.T.C. 1, 16 (2004). Under this framework, "[o]ur task is to determine whether the [Complaint] contains sufficient factual matter . . . to state a claim to relief that is plausible on its face." *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. 2010) (citation omitted). For purposes of this analysis, we "accept[] the allegations in the complaint as true and construe them in the light most favorable to [Complaint Counsel]." *Am. Dental Ass'n v. Cigna Corp.*, 605 F.3d 1283, 1288 (11th Cir. 2010).

ANALYSIS

I. THE COMMISSION HAS AUTHORITY TO ENFORCE THE FTC ACT BY ADJUDICATING WHETHER THE DATA SECURITY PRACTICES ALLEGED IN THE COMPLAINT ARE "UNFAIR."

LabMD contends that the Commission lacks statutory authority to regulate or bring enforcement action with respect to the data security practices alleged. Motion at 9-21. We disagree. As discussed below, the Commission's authority to protect consumers from unfair practices relating to deficient data security measures is well-supported by the FTC Act, is fully consistent with other statutes, and is confirmed by extensive case law.[4]

A. Congress Intended to Delegate Broad Authority to the Commission to Proscribe Activities that Qualify as "Unfair Acts or Practices."

LabMD's broadest argument is that Section 5 does not authorize the FTC to address *any* data security practices. *See, e.g.*, Motion at 10 ("even if Section 5 does authorize the FTC to

[3] The Commission's administrative adjudicatory proceedings are governed by the FTC Act and the Commission's Rules of Practice, rather than the rules and standards that govern federal courts. Nonetheless, "since many adjudicative rules are derived from the Federal Rules of Civil Procedure, the latter may be consulted for guidance and interpretation of Commission rules where no other authority exists." FTC Op. Manual § 10.7. Here, the most relevant provision in the Commission's Rules of Practice (16 C.F.R. § 3.11(b)(2)) is very similar to the analogous court rule (Fed. R. Civ. P. 8(a)(2)). Thus, in this instance, we exercise our discretion to apply the pleading standards summarized above.

[4] At some points in the Motion, LabMD frames its arguments as challenges to the scope of the Commission's "jurisdiction" (*e.g.*, at 1, 2, 8, 16, 18, 19), while elsewhere it acknowledges the Commission's "Section 5 'unfairness' authority" but asserts that we cannot apply such authority to LabMD's data security practices. *Id.* at 18. As the Supreme Court recently clarified, "there is *no difference*, insofar as the validity of agency action is concerned, between an agency's exceeding the scope of its authority (its 'jurisdiction') and its exceeding authorized application of authority that it unquestionably has." *City of Arlington v. FCC*, 133 S. Ct. 1863, 1870 (2013). This is because, "for agencies charged with administering congressional statutes[,] [b]oth their power to act and how they are to act is authoritatively prescribed by Congress." *Id.* at 1869; *see* Motion at 9.

regulate data-security, which it does not"); *id.* at 17 (asserting "the Commission's lack of power to regulate data security through its general Section 5 'unfairness' authority'"). Motion at 16. LabMD points out that "there is nothing in Section 5 explicitly authorizing the FTC to directly regulate . . . data-security practices." *Id.* at 20. Ignoring the facially broad reach of Section 5's prohibition of "unfair . . . acts or practices in or affecting commerce," LabMD urges the Commission to conclude from the absence of explicit "data security" authority in the FTC Act that the Commission has no such authority. *See, e.g.*, Motion at 14 ("When Congress has wanted the FTC to have data security authority, it has said so"); *id.* ("However, Congress has never given the Commission such authority and has, in fact, repeatedly made it clear that the FTC's power is very limited in application and very narrow in scope."); *id.* at 16 ("Section 5 does not give the FTC the authority to regulate data-security practices as 'unfair' acts or practices"); *id.* at 21 ("Section 5 does not contain a clear and manifest statement from Congress to authorize the Commission's [authority over] data security"). The statutory text, legislative history, and nearly a century of case law refute LabMD's argument.

As the courts have long recognized, "[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). Rather, the legislative history of the FTC Act confirms that Congress decided to delegate broad authority "to the [C]ommission to determine what practices were unfair," rather than "enumerating the particular practices to which [the term 'unfair'] was intended to apply. . . . There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." *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)). *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)).

This legislative history pertains to Congress' enactment of the prohibition of "unfair methods of competition" in 1914. Similar considerations motivated Congress's reuse of the same broad term ("unfair") when it amended the statute in 1938 to proscribe "unfair and deceptive acts and practices" as well as "unfair methods of competition." The 1938 amendment perpetuated and expanded the broad congressional delegation of authority to the Commission by "overturn[ing] . . . attempts [in some court decisions] to narrowly circumscribe the FTC's authority." *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 966 (D.C. Cir. 1985). Congress thus clarified that "the Commission can prevent such acts or practices which injuriously affect the general public as well as those which are unfair to competitors." *Id.* (quoting H.R. Rep. No. 1613, 75th Cong., 1st Sess. 3 (1937)).

As LabMD points out (*see* Motion at 18), Congress enacted legislation in 1994 that provided a sharper focus for the application of the Commission's "unfairness" authority, by amending the FTC Act to incorporate three specific criteria governing the application of "unfair . . . acts or practices" in adjudicatory and rulemaking proceedings. Specifically, the new Section 5(n) of the Act provides that, in enforcement actions or rulemaking proceedings, 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). These criteria, derived from the Commission's pre-existing *Policy Statement on Unfairness*, codified the analytical framework that the Commission already had been applying for the preceding decade in its efforts to combat "unfair . . . acts or practices." *See* Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980) ("*Policy Statement on Unfairness*"), *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1070, 1073 (1984). Section 5(n)'s specific criteria provide greater certainty for businesses by setting forth the factors to be used to evaluate whether their acts or practices are "unfair." That fact alone refutes LabMD's contention that the "general statutory terms" in Section 5 are too "vague" to be applied to the conduct alleged in the Complaint. *See* Motion at 19.

At the same time, Congress, in enacting Section 5(n), confirmed its intent to allow the Commission to continue to ascertain, on a case-by-case basis, which specific practices should be condemned as "unfair." Thus, to this day, "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." *Am. Fin. Servs. Ass'n*, 767 F.2d at 966.

The Commission and the federal courts have been applying these three "unfairness" factors for decades and, on that basis, have found a wide range of acts or practices that satisfy the applicable criteria to be "unfair," even though – like the data security practices alleged in this case – "there is nothing in Section 5 explicitly authorizing the FTC to directly regulate" such practices (*see* Motion at 20). *See, e.g., FTC v. Neovi, Inc.*, 604 F.3d 1150, 1155 (9th Cir. 2010) (creating and delivering 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); *Am. Fin. Servs. Ass'n*, 767 F.2d at 971 (oppressive litigation conduct to repossess household goods sold on credit).

LabMD cites *American Bar Association v. FTC*, 430 F.3d 457 (D.C. Cir. 2005), for the proposition that the Commission is overstepping the bounds of its authority to interpret the FTC Act. *See* Motion at 20. But that case is inapposite. *ABA* concerned the agency's determination, in construing the Gramm-Leach-Bliley Act ("GLB Act"), that attorneys fell within that statute's definition of "financial institutions" – a defined term that, in turn, incorporated by reference a set of lengthy and detailed definitions imported from other statutes and other agencies' regulations. The court found it "difficult to believe" that, in enacting a statutory "scheme of the length, detail, and intricacy of the one" under review, Congress could have left sufficient remaining ambiguity, "hidden beneath an incredibly deep mound of specificity," to support imposing GLB Act requirements upon "a profession never before regulated by federal [financial service] regulators, and never mentioned in the statute." 430 F.3d at 469. By contrast, the statutory text at issue in this case – "unfair . . . acts or practices" – conveys a far broader scope of interpretive flexibility, particularly given that this term is at the core of the Commission's own organic statute, the FTC Act.

LabMD similarly invokes *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000), for the proposition that "simple 'common sense as to the manner in which Congress is likely to delegate a policy decision of such economic and political magnitude' . . . reinforces the conclusion that the FTC lacks the authority to regulate the acts or practices alleged in the Complaint." Motion at 19 (quoting *Brown & Williamson*, 529 U.S. at 133). But *Brown & Williamson* is inapposite as well. In that case, the Court found that the Food and Drug Administration's attempts to regulate tobacco products conflicted directly with concrete manifestations of congressional intent. In particular, the Court concluded that, if the FDA had the authority it claimed, its own findings would have compelled it to ban tobacco products outright, whereas various tobacco-related statutes made clear that Congress wished *not* to ban such products. *See* 529 U.S. at 137-39. Here, of course, LabMD can cite no similar congressional intent to preserve inadequate data security practices that unreasonably injure consumers.

Similarly, the Court found that "Congress' specific intent when it enacted the FDCA" (Food, Drug & Cosmetics Act) in 1938 was to deny the FDA authority to regulate tobacco products. 529 U.S. at 146. The Court reasoned that, "*given the economic and political significance of the tobacco industry at the time*, it is extremely unlikely that Congress could have intended to place tobacco within the ambit of the FDCA absent any discussion of the matter." *Id.* at 147 (emphasis added).[5] By contrast, when enacting the FTC Act in 1914 and amending it in 1938, Congress had no way of anticipating the "economic and political significance" of data security practices in today's online environment. Accordingly, the fact that "there is no evidence in the text of the [FTC Act] or its legislative history that Congress in 1938 even considered the applicability of the Act" to data security practices is completely irrelevant. Congress could not possibly have had any "specific intent" to deny the FTC authority over data security practices. It did, however, intend to delegate broad authority to the FTC to address emerging business practices – including those that were unforeseeable when the statute was enacted. That is the only congressional intent that matters here.

B. The Commission Has Consistently Affirmed Its Authority under the FTC Act to Take Enforcement Action against Unreasonable Data Security Activities that Qualify as Unfair Acts and Practices

LabMD similarly attempts to draw support from the *Brown & Williamson* Court's determination that the FDA's 1996 "assertion of authority to regulate tobacco products" contradicted the agency's previous "consistent and repeated statements [over the preceding 73 years] that it lacked authority . . . to regulate tobacco absent claims of therapeutic benefit by the manufacturer," and the Court's conclusion that congressional enactments "against the backdrop" of the FDA's historic disavowal of authority confirmed that Congress did not intend to authorize such regulation. 529 U.S. at 132, 144-46. LabMD argues, by analogy, that "the Commission

[5] As the D.C. Circuit has recently recognized, these considerations are essential to the holding of *Brown & Williamson*, and, in their absence, that case does not justify restricting agency action under a broad statutory mandate. *See Verizon v. FCC*, No. 11-1355, at 23-25 (D.C. Cir., Jan. 14, 2014) (slip op.).

[previously] did not claim Section 5 'unfairness' authority to regulate patient-information (or any other) data-security practices," but "recently reversed course without explanation," thus purportedly defying congressional intent. Motion at 16, 18.

That analogy, too, is without merit. Unlike the FDA, the Commission has never disavowed authority over online privacy or data security matters. To the contrary, "[t]he Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace," and has repeatedly and consistently affirmed its authority to challenge unreasonable data security measures as "unfair . . . acts or practices" in violation of Section 5. *See* FTC Report to Congress, *Privacy Online*, at 2 (June 1998) ("*1998 Online Privacy Report*").[6] LabMD cites out-of-context snippets from the Commission's 1998 and 2000 reports to Congress for the unfounded proposition that, at that time, the Commission believed its authority over data security matters was "limited to ensuring that Web sites follow their stated information practices."[7] LabMD's characterization does not withstand scrutiny. Neither the text it quotes nor the reports as a whole can plausibly be read as disavowing the Commission's authority to take enforcement action against data security practices that violate Section 5's prohibition of "unfair . . . acts or practices," as defined in Section 5(n). Indeed, the Commission clearly stated that certain conduct relating to online data security is "likely to be an unfair practice," and, in both reports, confirmed its view that the FTC Act "provides a basis for government enforcement" against information practices [that] may be inherently . . . unfair, regardless of whether the entity has publicly adopted any fair information practice policies."[8] In context, the sentences from the 1998 and 2000 reports relied upon by LabMD simply recognize that the Commission's existing authority may not be sufficient to effectively protect consumers with regard to *all* data privacy issues of potential concern (such as aspects of children's online privacy) and that expanded rulemaking authority and enforcement remedies could enhance the Commission's ability to meaningfully address a broader range of such concerns.[9] The same

---

[6] *See* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[7] Motion at 16 n.12 (quoting *1998 Online Privacy Report* at 41) ("As a general matter, the Commission lacks authority to require firms to adopt information practice policies."); Reply at 7-8 (quoting FTC Report to Congress, *Privacy Online: Fair Information Practices in the Electronic Age* (May 2000) ("*2000 Online Privacy Report*") (http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf) ("As a general matter, . . . 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").

[8] *1998 Online Privacy Report* at 12-13, 40-41. *See also 2000 Online Privacy Report* at 33-34 ("The Commission's authority over the collection and dissemination of personal data collected online stems from Section 5[,]" which "prohibits unfair and deceptive practices in and affecting commerce," and thus "authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of the Act, and provides a basis for government enforcement of certain [norms concerning] fair information practices").

[9] *See 1998 Online Privacy Report* at 42 (recognizing that "Section 5 may only have application to some but not all practices that raise concern about the online collection and use of information from children," and recommending legislation authorizing the Commission to promulgate "standards of practice governing the online collection and use of information from children."); *2000 Online Privacy Report* at

error infects LabMD's mischaracterization of testimony that Commissioners and high-level Commission staff members delivered to various congressional committees and subcommittees.[10]

Since the late 1990s, the Commission has repeatedly affirmed its authority to take action against unreasonable data security measures as "unfair . . . acts or practices" in violation of Section 5, in reports, testimony to Congress, and other publicly-released documents.[11] The Commission has also confirmed this view by bringing 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. For example, on May 1, 2006, the Commission filed a complaint in the U.S. District Court for the District of Wyoming, charging that defendant Accusearch, Inc. and its principal obtained consumers' private information (specifically, data concerning their telecommunications usage) and caused such data to be disclosed to unauthorized third parties without consumers' knowledge or consent. *FTC v. Accusearch, Inc.*, Case No. 2:06-cv-0105, Complaint, at ¶¶ 9-13. The Commission alleged that this conduct was "an unfair practice in violation of Section 5(a) of the FTC Act," *id.*, ¶ 14, because it "caused or [was] likely to cause substantial injury to consumers that [was] not reasonably avoidable by consumers and [was] not outweighed by

---

36-37 (seeking legislation granting "authority to promulgate more detailed standards pursuant to the Administrative Procedure Act," including "rules or regulations [that] could provide further guidance to Web sites by defining fair information practices with greater specificity[,]"such as "what constitutes 'reasonable access' and 'adequate security'"). *See also* Motion at 17 n.13 (quoting same).

[10] *See* Motion at 16-17, nn.12, 13, 14 (citing testimony by Chairman Robert Pitofsky in 1998, then-Commissioner Edith Ramirez in 2011, Chairman Jonathan Leibowitz in 2012, and Bureau Directors Eileen Harrington and David Vladeck in 2009 and 2011, respectively). In such testimony, the FTC representatives conveyed the Commission's support for draft data security legislation that would expand the FTC's *existing* authority by providing it with rulemaking authority under the Administrative Procedure Act and civil penalty authority. *See, e.g.*, Prepared Statement of the FTC, *Data Security*, presented by Commissioner Edith Ramirez to House Comm. on Energy & Commerce, Subcomm. on Commerce, Mfg., and Trade, at 11-12 (June 5, 2011) (http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf).

[11] *See, e.g.*, Prepared Statement of the FTC, *Identity Theft: Innovative Solutions for an Evolving Problem*, presented by Bureau Dir. Lydia B. Parnes to Senate Comm. on the Judiciary, Subcomm. on Terrorism, Tech., and Homeland Security, at 5-6 (Mar. 21, 2007) (http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-identity-theft-innovative-solutions-evolving-problem/p065409identitytheftsenate03212007.pdf); FTC Staff Report, *Protecting Consumers in the Next Tech-ade*, at 29-30 (Spring 2008) (http://www.ftc.gov/sites/default/files/documents/reports/protecting-consumers-next-tech-ade-report-staff-federal-trade-commission/p064101tech.pdf); FTC Report, *Security in Numbers, SSNs and ID Theft*, at 7 (Dec. 2008) (http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf); Prepared Statement of the FTC, *Protecting Social Security Numbers From Identity Theft*, presented by Assoc. Bureau Dir. Maneesha Mithal to House Comm. on Ways and Means, Subcomm. on Soc. Security, at 8 (April 13, 2011) (http://ftc.gov/os/testimony/110411ssn-idtheft.pdf); FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change*, at 14, 73 (March 26, 2012) (http://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers). *See also* note 13, *infra*.

countervailing benefits to consumers or competition." *Id.*, ¶ 13. The district court agreed, granting summary judgment to the Commission in 2007, and the Tenth Circuit affirmed in 2009. *See Accusearch*, *supra*, 570 F.3d 1187. Since then, the Commission has taken the same position in dozens of other enforcement proceedings, including administrative adjudications,[12] as well as complaints filed in federal courts, *see* CC Opp. at 12-13 n.9 (citing cases). In these cases, the Commission challenged allegedly unreasonable data security measures (or other practices that enabled unauthorized third parties to harm consumers by obtaining access to their confidential personal data) as "unfair acts or practices" in violation of Section 5. And in each case, it clearly reaffirmed its position that it possessed jurisdiction over the allegedly "unfair" data security practices under Section 5.

The fact that the Commission initially focused its enforcement efforts primarily on "deceptive" data security practices, and began pursuing "unfair" practices in 2005, does not mean that the Commission lacked jurisdiction over "unfair" practices before then. As then-Commissioner Orson Swindle testified to a House subcommittee in 2004, "To date, the Commission's security cases have been based on its authority to prevent deceptive practices," but it "also has authority to challenge practices as unfair if they cause consumers substantial injury that is neither reasonably avoidable nor offset by countervailing benefits. The Commission has used this authority in appropriate cases to challenge a variety of injurious practices, including unauthorized charges in connection with 'phishing.'"[13] LabMD cites Commissioner Swindle's reference to the Commission's "deceptiveness" authority over data security practices, *see* Motion at 16 n.12, but neglects to mention his reference to the Commission's "unfairness" authority over such practices.

LabMD also misinterprets the Commission's expressions of support for legislation relating to data security as requests for authority to fill regulatory "gaps" that it could not fill without such legislation. *Id.* at 17 & nn.13, 14. LabMD refers to three data security-related laws that the Commission supported, and that Congress ultimately enacted – *i.e.*, the GLB Act,[14] the

---

[12] *See BJ's Wholesale Club, Inc.*, 140 F.T.C. 465, 470 (2005); *DSW, Inc.*, 141 F.T.C. 117, 122 (2006); *CardSystems Solutions, Inc.*, Docket No. C-4168, 2006 WL 2709787, *3 (Sept. 5, 2006); *Reed Elsevier, Inc.*, Docket No. C-4226, 2008 WL 3150420, *4 (July 29, 2008); *TJX Cos., Inc.*, Docket No. C-4227, 2008 WL 3150421, *3 (Sept. 29, 2008). In these and similar cases, the Commission issues its final Decisions & Orders only after placing the relevant proposed consent orders on the public record, issuing Notices in the Federal Register that summarize and explain the provisions of the proposed orders and invite public comment, and considering comments filed by interested members of the public. *See* 16 C.F.R. § 2.34(c) & (e).

[13] Prepared Statement of the FTC, *Protecting Information Security and Preventing Identity Theft*, presented by Commissioner Orson Swindle to House Comm. on Gov't Reform, Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census, at 7, 14 n.24 (Sept. 22, 2004) (http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-information-security-and-preventing-identity/040922infosecidthefttest.pdf) ("*Comm'r Swindle's 2004 Information Security Testimony*").

[14] Pub. L. 106-102 (1999) (codified in pertinent part at 15 U.S.C. § 6804(a)(1)).

Children's Online Privacy Protection Act ("COPPA"),[15] and the Fair and Accurate Credit Transactions Act of 2003 ("FACTA").[16] But these laws *recognized* the Commission's *existing* enforcement authority, *expanded* that authority in particular respects, and affirmatively *directed* the Commission to take particular actions to protect consumer interests in specified contexts. For example, in COPPA, Congress authorized the Commission to sue for civil penalties in addition to the equitable monetary relief available under existing law, and authorized and directed the Commission to promulgate rules to protect children's online privacy pursuant to the streamlined procedures of the Administrative Procedure Act ("APA"), rather than using the more time-consuming procedures mandated by Section 18 of the FTC Act, 15 U.S.C. § 57a. Similarly, in both FACTA and the GLB Act, Congress directed the Commission to adopt rules addressing specified topics using streamlined APA procedures; and in FACTA, Congress also expanded the range of remedies available in Commission enforcement actions.

Finally, even if they were otherwise plausible, LabMD's arguments about the intended meaning of the past statements of the Commission or its members or staff would still be immaterial to the ultimate question of the Commission's statutory authority. "An agency's initial interpretation of a statute that it is charged with administering is not 'carved in stone,'" and agencies "must be given ample latitude to 'adapt their rules and policies to the demands of changing circumstances." *Brown & Williamson*, 529 U.S. at 156-57 (quoting *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 863 (1984); *Smiley v. Citibank (S.D.)*, 517 U.S. 735, 742 (1996); *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 42 (1983); and *Permian Basin Area Rate Cases*, 390 U.S. 747, 784 (1968)); *see also Verizon v. FCC*, *supra* note 5, at 19-20. Presented with the concrete circumstances of this case, the Commission concludes that it can and should address whether or not LabMD's data security procedures constitute "unfair . . . acts or practices" within the meaning of the FTC Act. To conclude otherwise would disregard Congress's instruction to the Commission to protect consumers from harmful practices in evolving technological and marketplace environments.

C. HIPAA and Other Statutes Do Not Shield LabMD from the Obligation to Refrain from Committing Unfair Data Security Practices that Violate the FTC Act.

Contrary to LabMD's contention, Congress has never enacted any legislation that, expressly or by implication, forecloses the Commission from challenging data security measures that it has reason to believe are "unfair . . . acts or practices." LabMD relies on numerous "targeted statutes" that Congress has enacted in recent years "specifically delegating" to the Commission or to other agencies "statutory authority over data-security" in certain narrower fields. Motion at 15. But LabMD has not identified a single provision in any of these statutes that expressly withdraws any authority from the Commission. Thus, its argument that these more specific statutes implicitly repeal the FTC's preexisting authority is unpersuasive. "The cardinal rule is that repeals by implication are not favored. Where there are two acts upon the same subject, effect should be given to both if possible." *Posadas v. Nat'l City Bank of N.Y.*,

[15] Pub. L. 105-277 (1998) (codified in pertinent part at 15 U.S.C. §§ 6502(b), 6505(d)).

[16] Pub. L. 108-159 (2003) (codified in pertinent part at 15 U.S.C. § 1681s(a)).

296 U.S. 497, 503 (1936). Thus, one cannot conclude that Congress implicitly repealed or narrowed the scope of an existing statute (*i.e.*, Section 5) by subsequently enacting a new law unless "the intention of the legislature to repeal [is] clear and manifest; otherwise, at least as a general thing, the later act is to be construed as a continuation of, and not a substitute for, the first act . . . ." *Id.*; *see also Branch v. Smith*, 538 U.S. 254, 273 (2003) ("An 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.'"); *Morton v. Moncari*, 417 U.S. 535, 551 (1974) ("when two statutes are capable of co-existence, it is the duty of the courts, absent a clearly expressed congressional intention to the contrary, to regard each as effective").

Nothing in HIPAA, HITECH,[17] or any of the other statutes LabMD cites reflects a "clear and manifest" intent of Congress to restrict the Commission's authority over allegedly "unfair" data security practices such as those at issue in this case. LabMD identifies no provision that creates a "clear repugnancy" with the FTC Act, nor any requirement in HIPAA or HITECH that is "clearly incompatible" with LabMD's obligations under Section 5. *See* Motion at 13. To the contrary, the patient-information protection requirements of HIPAA are largely consistent with the data security duties that the Commission has enforced pursuant to the FTC Act. Indeed, the FTC and the Department of Health and Human Services ("HHS") have worked together "to coordinate enforcement actions for violations that implicate both HIPAA and the FTC Act." HHS, *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules*, Final Rule, 78 Fed. Reg. 5566, 5579 (Jan. 25, 2013). And the two agencies have obtained favorable results by jointly investigating the data security practices of companies that may have violated each of these statutes.[18]

LabMD further argues that HIPAA's comprehensive framework governing "patient-information data-security practices" by HIPAA-regulated entities somehow trumps the

---

[17] *See* Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. 104-191 (1996) (codified in pertinent part at 42 U.S.C. §§ 1320d *et seq.*); American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, Div. A, Title XIII, and Div. B, Title IV ("Health Information Technology for Economic and Clinical Health Act") ("HITECH") (codified at 42 U.S.C. §§ 1320d-5 *et seq.*).

[18] For example, in 2009, CVS Caremark simultaneously settled HHS charges of HIPAA violations and FTC charges of FTC Act violations, stemming from the two agencies' coordinated investigations of the company's failure to securely dispose of documents containing consumers' sensitive financial and medical information. *See* FTC Press Release: *CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations* (Feb. 18, 2009) (http://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial); *CVS Caremark Corp.*, Consent Order, FTC Docket No. C-4259, 2009 WL 1892185 (June 18, 2009). *See also* HHS Press Release: *CVS Pays $2.25 Million and Toughens Practices to Settle HIPAA Privacy Case* (Feb. 18, 2009) (http://www.hhs.gov/news/press/2009pres/02/20090218a.html). Similarly, in 2010, Rite Aid entered consent decrees to settle both FTC charges of FTC Act violations and HHS charges of HIPAA violations, which the two agencies had jointly investigated. *See Rite Aid Corp.*, Consent Order, 150 F.T.C. 694 (2010); HHS Press Release: Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case (July 27, 2010) (http://www.hhs.gov/news/press/2010pres/07/20100727a.html).

application of the FTC Act to that category of practices. Motion at 11-12. But HIPAA evinces no congressional intent to preserve anyone's ability to engage in inadequate data security practices that unreasonably injure consumers in violation of the FTC Act, and enforcement of that Act thus fully comports with congressional intent under HIPAA. LabMD similarly contends that, by enacting HIPAA, Congress vested HHS with "exclusive administrative and enforcement authority with respect to HIPAA-covered entities under these laws." *Id.* at 11. That argument is also without merit. To be sure, the Commission cannot enforce HIPAA and does not seek to do so.[19] But nothing in HIPAA or in HHS's rules negates the Commission's authority to enforce the FTC Act.[20]

Indeed, the FTC Act makes clear that, when Congress wants to exempt a particular category of entities or activities from the Commission's authority, it knows how to do so explicitly – further undermining LabMD's claim to an implicit "carve-out" from the Commission's jurisdiction over HIPAA-covered entities or their "patient-information data security practices." Section 5(a)(2) specifically lists categories of businesses whose acts and practices are not subject to the Commission's authority under the FTC Act. These include banks, savings and loans, credit unions, common carriers subject to the Acts to regulate commerce, air carriers, and entities subject to certain provisions in the Packers and Stockyards Act of 1921. 15 U.S.C. § 45(a)(2). Congress could have added "HIPAA-covered entities" to that list, but it did not. Similarly, the statute identifies certain types of practices that the Commission may not address, such as commerce with foreign nations in certain circumstances. *Id.* § 45(a)(3). But it provides no carve-out for data security practices relating to patient information, to which HIPAA may apply.

LabMD relies on *Credit Suisse Securities, LLC v. Billing*, 551 U.S. 264 (2007), for the proposition that industry-specific requirements in other statutes may trump more general laws such as the FTC Act. *See* Motion at 13. *Credit Suisse* is clearly distinguishable. As LabMD concedes, there was a "possible conflict between the [securities and antitrust] laws," creating a "risk that the specific securities and general antitrust laws, if both applicable, would produce conflicting guidance, requirements, . . . or standards of conduct." *Id.* By contrast, nothing in the

[19] LabMD repeatedly – but incorrectly – asserts that "the FTC agrees that LabMD has not violated HIPAA or HITECH." *See, e.g.*, Motion at 13; *see also* Reply at 4 ("a company FTC admits *complied* with HIPAA/HITECH in all respects") (emphasis in original); *id.* at 5 ("FTC admits LabMD has always complied with all applicable data-security regulations"); *id.* at 12 ("FTC *admits* that LabMD, a HIPAA-covered entity, always complied with HIPAA/HITECH regulations") (emphasis in original). The Commission does not enforce HIPAA or HITECH, and has never expressed any view on whether LabMD has, or has not, violated those statutes.

[20] Both HHS (pursuant to HIPAA and HITECH) and the FTC (pursuant to the American Recovery and Reinvestment Act of 2009) have promulgated regulations establishing largely congruent requirements concerning notification of data breaches involving consumers' private health information, but they are applicable to two different categories of firms. *Compare* 16 C.F.R. Part 318 (FTC rule) *with* 45 C.F.R. Part 164, Subparts D & E (HHS rule). LabMD correctly notes that this FTC rule does not apply to HIPAA-covered entities, *see* Motion at 12 & n.9, but the conclusion it draws from this fact is unfounded. Significantly, the Complaint in the present proceeding alleges only statutory violations; it does not allege violations of the FTC's Health Breach Notification Rule.

FTC Act compels LabMD to engage in practices forbidden by HIPAA, or vice versa. It is not unusual for a party's conduct to be governed by more than one statute at the same time, as "we live in 'an age of overlapping and concurrent regulatory jurisdiction[.]'" *FTC v. Ken Roberts Co.*, 276 F.3d 583, 593 (D.C. Cir. 2001) (quoting *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192 (D.C. Cir. 1996)). LabMD and other companies may well be obligated to ensure their data security practices comply with both HIPAA and the FTC Act. But so long as the requirements of those statutes do not conflict with one another, a party cannot plausibly assert that, because it complies with one of these laws, it is free to violate the other. Indeed, courts have consistently ruled that "the FTC may proceed against unfair practices even if those practices [also] violate some other statute that the FTC lacks authority to administer." *Accusearch*, 570 F.3d at 1194-95 (concluding that conduct may be an unlawful "unfair . . . act or practice" under the FTC Act even if it also violates the Telecommunications Act of 1996). *See also Orkin Exterminating Co.*, 849 F.2d at 1353 (rejecting proposition that a "mere breach of contract . . . is outside the ambit of [the "unfairness" prohibition in] section 5"); *Am. Fin. Servs. Ass'n*, 767 F.2d at 982-83 (FTC may ban certain creditor remedies, such as wage assignments and repossession of consumers' household goods, as "unfair . . . acts or practices" under the FTC Act, even where such conduct also ran counter to state laws against enforcing unconscionable contracts of adhesion).

Finally, LabMD argues that Congress' enactment of three new statutes addressing the Commission's authority over certain data protection matters in discrete contexts implies that Congress must have believed that, in other respects, the Commission lacked statutory authority to address data protection matters under the FTC Act. That argument, too, is without merit. First, as discussed above, in each of these statutes Congress *expanded* the enforcement and rulemaking tools that the Commission *already* possessed for addressing data security problems in discrete areas. *See supra* at 8 n.10, 9-10. LabMD identifies nothing in any of those bills or their legislative histories indicating that the Commission's authority to enforce Section 5's prohibition of "unfair . . . acts or practices" was limited in any way. Moreover, these statutes affirmatively *directed* the Commission to take particular actions to protect consumer interests in specified contexts.[21] Of course, by *compelling* the Commission to take particular steps in those contexts, Congress did not somehow divest the Commission of its preexisting and much broader *authority* to protect consumers against "unfair" practices. Congress commonly authorizes agencies to oversee entire fields while specifying, in a few areas, what minimum steps those agencies must take in exercising that authority, and the enumeration of those minimum steps does not cast doubt on the agencies' broader authority. *See, e.g.*, *Cablevision Sys. Corp. v. FCC*, 649 F.3d 695, 705-06 (D.C. Cir. 2011). And LabMD's reliance on data security-related bills that ultimately were *not* enacted into law (*see* Motion at 17-18 & n.15; Reply at 9) contradicts basic principles of statutory interpretation.[22]

[21] For example, in COPPA, Congress directed the Commission to promulgate rules addressing the specific duties of child-directed website operators to provide specific notices and obtain parental consent before collecting or disclosing children's personal information. *See* 15 U.S.C. § 6502(b).

[22] The fact that a proposed bill was not enacted into law does not mean that Congress consciously "rejected" it. Enacting a bill into law is a notoriously difficult and time-consuming process, given the procedural and political hurdles to be overcome before obtaining majority votes of both Houses of Congress, reconciliation of any differences between the two Houses' versions, and signature by the President. Thus, "the fact that Congress has considered, but failed to enact, several bills" typically sheds

In sum, we reject LabMD's contention that the Commission lacks authority to apply the FTC Act's prohibition of "unfair . . . acts or practices" to data security practices, in the field of patient information or in other contexts; and we decline to dismiss the Complaint on that basis.

II. THE COMMISSION HAS AUTHORITY TO ENFORCE THE STATUTE BY ADJUDICATING ALLEGED VIOLATIONS, DESPITE THE ABSENCE OF REGULATIONS, WITHOUT INFRINGING LABMD'S DUE PROCESS RIGHTS.

A. Administrative Agencies May Interpret and Enforce Statutory Requirements in Case-by-Case Adjudications, as Well as By Rulemaking.

LabMD argues that the Commission may not adjudicate whether the alleged conduct violated Section 5 of the FTC Act because the Commission "has not prescribed regulations or legislative rules under Section 5 establishing patient-information (or any other) data-security standards that have the force of law." Motion at 23. LabMD asserts that "[t]he FTC's refusal to issue regulations is wrongful and makes no sense." *Id.* at 24. LabMD's position conflicts with longstanding case law confirming that administrative agencies may – indeed, must – enforce statutes that Congress has directed them to implement, regardless whether they have issued regulations addressing the specific conduct at issue. Thus, in the leading case of *SEC v. Chenery*, the Supreme Court recognized that the SEC had not exercised its statutory rulemaking authority with regard to the matter at issue, and squarely rejected the contention "that the failure of the Commission to anticipate this problem and to promulgate a general rule withdrew all power from that agency to perform its statutory duty in this case." 332 U.S. 194, 201-02 (1947). To the contrary: "the Commission had a statutory duty to decide the issue at hand in light of the proper standards[,] and . . . this duty remained 'regardless of whether those standards previously had been spelled out in a general rule or regulation.'" *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 292 (1974) (quoting *Chenery*, 332 U.S. at 201).

The Commission has long recognized that "information security is an ongoing process of assessing risks and vulnerabilities: no one static standard can assure appropriate security, as security threats and technology constantly evolve." *See Comm'r Swindle's 2004 Information Security Testimony* at 3. Such complex questions relating to data security practices in an online environment are particularly well-suited to case-by-case development in administrative adjudications or enforcement proceedings, given the difficulty of drafting generally applicable regulations that fully anticipate the concerns that arise over emerging business arrangements in this rapidly changing area. As the Supreme Court has explained,

---

little, if any, light on what Congress believed or intended; and the adjudicator's "task . . . is not to construe bills that Congress has failed to enact, but to construe statutes that Congress has enacted." *Wright v. West*, 505 U.S. 277, 294 n.9 (1992) (Thomas, J.) (plurality op.); *see also Verizon v. FCC*, *supra* note 5, at 25 ("pieces of subsequent failed legislation tell us little if anything about the original meaning" of a statute, and thus such later, unenacted legislative proposals provide "an unreliable guide to legislative intent") (citations omitted).

> [P]roblems 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. There is thus a very definite place for the case-by-case evolution of statutory standards. And the choice made between proceeding by general rule or by individual, ad hoc litigation is one that lies primarily in the informed discretion of the administrative agency.

Chenery, 332 U.S. at 202-03. Accordingly, "agency discretion is at its peak in deciding such matters as whether to address an issue by rulemaking or adjudication[,] [and] [t]he Commission seems on especially solid ground in choosing an individualized process where important factors may vary radically from case to case." *American Gas Ass'n v. FERC*, 912 F.2d 1496, 1519 (D.C. Cir. 1990). *See also 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).

The Commission has enforced Section 5's prohibition of "unfair . . . acts or practices" primarily through case-by-case adjudication and litigation from the time the statute was enacted. Indeed, numerous recent cases have condemned conduct that facilitated identity theft or involved misuse of confidential consumer information as unlawful "unfair . . . acts or practices," although the practices were unprecedented and not covered by any preexisting rules. Thus, even though the Commission had never promulgated any regulations governing the creation of online checks or bank drafts without adequate verification procedures, the Ninth Circuit, in *Neovi*, easily affirmed both the district court's holding that the defendants had committed "unfair acts or practices," 604 F.3d at 1155-58, and its requirement that the defendants disgorge all revenue from the unlawful conduct. *Id.* at 1159-60. Similarly, despite the absence of any regulation prohibiting online data brokers from gathering and selling consumers' confidential information gleaned from telephone records, the Tenth Circuit affirmed a district court decision finding that the defendants' conduct constituted "unfair acts and practices" and imposing an equitable disgorgement remedy. *See generally Accusearch*, 570 F.3d 1187.

B. This Proceeding Respects LabMD's Due Process Rights

The Commission's decision to proceed through adjudication without first conducting a rulemaking also does not violate LabMD's constitutional due process rights. The courts have rejected such due process challenges to agency adjudications on numerous occasions. For example, in *Gonzalez v. Reno*, 212 F.3d 1338 (11th Cir. 2000), the court held that the agency did not violate due process in interpreting and implementing the immigration statute in an

enforcement proceeding, even though its "policy was developed in the course of an informal adjudication, rather than during formal rulemaking." 212 F.3d at 1350. *See also Taylor v. Huerta*, 723 F.3d 210, 215 (D.C. Cir. 2013) (statute enabling agency to revoke pilot's license following administrative adjudicatory proceeding "represented nothing more than an ordinary exercise of Congress' power to decide the proper division of regulatory, enforcement, and adjudicatory functions between agencies in a split-enforcement regime . . . . [Petitioner] cites no authority, and presents no persuasive rationale, to support his claim that due process requires more."); *RTC Transp., Inc. v. ICC*, 731 F.2d 1502, 1505 (11th Cir. 1984) (rejecting contention that agency's "application of its policy . . . denied them due process because the policy was announced in adjudicatory proceedings, . . . rather than being promulgated in rulemaking proceedings with notice and opportunity for comment"); *Shell Oil Co. v. FERC*, 707 F.2d 230, 235-36 (5th Cir. 1983) (noting that parties in administrative adjudicatory proceedings are not denied due process even when agencies establish new, binding standards of general application in such proceedings, so long as affected parties are given meaningful opportunities to address the factual predicates for imposing liability).

To be sure, constitutional due process concerns may arise if the government imposes criminal punishment or civil penalties for past conduct (or unduly restricts expression protected by the First Amendment) pursuant to a law that "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012) (quoting *United States v. Williams*, 553 U.S. 285, 304 (2008)). But, as the D.C. Circuit held in rejecting a constitutional due process challenge to the Commission's implementation of the Fair Credit Reporting Act,

> [E]conomic regulation is subject to a less strict vagueness test because its subject matter is often more narrow, and because businesses, which face economic demands to plan behavior carefully, can be expected to consult relevant legislation in advance of action. The regulated enterprise . . . may have the ability to clarify the meaning of the regulation by its own inquiry, or by resort to an administrative process. Finally, the consequences of imprecision are qualitatively less severe when laws have . . . civil rather than criminal penalties.

Trans Union Corp. v. FTC, 245 F.3d 809, 817 (D.C. Cir. 2001) (quoting *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498-99 (1982)).

Here, the three-part statutory standard governing whether an act or practice is "unfair," set forth in Section 5(n), should dispel LabMD's concern about whether the statutory prohibition of "unfair . . . acts or practices" is sufficient to give fair notice of what conduct is prohibited. In enacting Section 5(n), Congress endorsed the Commission's conclusion that "the unfairness standard is the result of an evolutionary process . . . . [that] must be arrived at by . . . a gradual process of judicial inclusion and exclusion." *Policy Statement on Unfairness*, 104 F.T.C. at 1072. This is analogous to the manner in which courts in our common-law system routinely develop or refine the rules of tort or contract law when applying established precedents to new

factual situations. 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 judicial decision in the common-law tradition." *Northwest Airlines, Inc. v. Transp. Workers Union of Am*., 451 U.S. 77, 95 (1981).

LabMD's due process claim is particularly untenable when viewed against the backdrop of the common law of negligence. Every day, courts and juries subject companies to tort liability for violating uncodified standards of care, and the contexts in which they make those fact-specific judgments are as varied and fast-changing as the world of commerce and technology itself. The imposition of such tort liability under the common law of 50 states raises the same types of "predictability" issues that LabMD raises here in connection with the imposition of liability under the standards set forth in Section 5(n) of the FTC Act. In addition, when factfinders in the tort context find that corporate defendants have violated an unwritten rule of conduct, they – unlike the FTC – can normally impose compensatory and even punitive damages. Even so, it is well-established that the common law of negligence does not violate due process simply because the standards of care are uncodified. There is similarly no basis to conclude that the FTC's application of the Section 5(n) cost-benefit analysis violates due process, particularly where, as here, the complaint does not even seek to impose damages, let alone retrospective penalties.

III. LABMD'S ALLEGED PRACTICES ARE "IN OR AFFECTING COMMERCE" UNDER THE FTC ACT

In Section III of the Motion to Dismiss, LabMD contends that the acts and practices alleged in the Complaint do not satisfy the statutory definition of "commerce" set forth in Section 4 of the FTC Act – *i.e.*, "commerce 'among' or 'between' states." *See* Motion at 28 (citing and paraphrasing 15 U.S.C. § 44, and asserting that LabMD's principal place of business is in Georgia; the alleged acts or practices were committed in Georgia; and its servers and computer network are located in Georgia). This argument is frivolous. The Complaint plainly alleges that LabMD "tests samples from consumers located throughout the United States." Complaint, ¶ 5; *see also* ¶ 2. Indeed, LabMD concedes in its Answer to the Complaint that it "tests samples . . . which may be sent from six states outside of Georgia: Alabama, Mississippi, Florida, Missouri, Louisiana, and Arizona." Answer, ¶ 5. Thus, the complaint unquestionably alleges that LabMD's acts and practices "have been in or affecting commerce, as 'commerce' is defined in Section 4[.]" Complaint, ¶ 2.

IV. THE ALLEGATIONS IN THE COMPLAINT STATE A PLAUSIBLE CLAIM THAT LABMD ENGAGED IN "UNFAIR . . . ACTS OR PRACTICES"

We turn next to LabMD's contention that "the Complaint does not state a plausible claim for relief" on the ground that the "Complaint's allegations are nothing more than inadequate 'legal conclusions couched as factual allegations.'" Motion at 28-29 (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 554, 555 (2007)).

That is incorrect. The Complaint quite clearly sets forth specific allegations concerning LabMD's conduct and other elements of the charged violation. In particular, it includes plausible

allegations that satisfy each element of the statutory standard for unfairness: that (1) the alleged conduct caused, or was likely to cause, substantial injury to consumers; (2) such injury could not reasonably have been avoided by consumers themselves; and (3) such injury was not outweighed by benefits to consumers or competition. 15 U.S.C. § 45(n). We emphasize that, for purposes of addressing LabMD's Motion to Dismiss, we presume – without deciding – that these allegations are true. But the Commission's ultimate decision on LabMD's liability will depend on the factual evidence to be adduced in this administrative proceeding.

A. Causation or Likely Causation of Substantial Injury to Consumers

The Complaint contains sufficient allegations to satisfy the criterion that the respondent's acts or practices "cause[d], or [were] likely to cause, substantial injury to consumers." *Id.* First, the Complaint alleges that LabMD collected and stored on its computer system highly sensitive information on consumers' identities (*e.g.*, names linked with addresses, dates of birth, Social Security numbers, and other information), their medical diagnoses and health status, and their financial transactions with banks, insurance companies, and health care providers. *See* Complaint, ¶¶ 6-9, 19, 21.

Second, the Complaint contains allegations that LabMD implemented unreasonable data security measures. These measures allegedly included (*i*) "acts of commission," such as installing Limewire, a peer-to-peer file sharing application, on a billing manager's computer, *see id.*, ¶¶ 13-19, as well as (*ii*) "acts of omission," such as failing to institute any of a range of readily-available safeguards that could have helped prevent data breaches. *See id.*, ¶¶ 10(a)-(g)).

Third, the Complaint alleges that LabMD's actions and failures to act, collectively, directly caused "substantial injury" resulting from both (*i*) actual data breaches, enabling unauthorized persons to obtain sensitive consumer information, *id.*, ¶¶ 17-21, as well as (*ii*) increased risks of other potential breaches. *Id.*, ¶¶ 11-12, 22. Notably, the Complaint's allegations that LabMD's data security failures led to *actual* security breaches, if proven, would lend support to the claim that the firm's data security procedures caused, or were likely to cause, harms to consumers – but the mere fact that such breaches occurred, standing alone, would not necessarily establish that LabMD engaged in "unfair . . . acts or practices." The Commission has long recognized that "the occurrence of a breach does not necessarily show that a company failed to have reasonable security measures. There is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution." *See Comm'r Swindle's 2004 Information Security Testimony* at 4.[23] Accordingly, we will need to determine whether the "substantial injury" element is satisfied by considering not only whether the facts alleged in the Complaint actually occurred, but also whether LabMD's data security procedures

[23] *See also In re SettlementOne Credit Corp.*, File No. 082 3209, Letter to Stuart K. Pratt, Consumer Data Industry Association, from Donald S. Clark, Secretary, by Direction of the Commission, at 2 (Aug. 17, 2011) (http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819lettercdia_1.pdf) (affirming, in resolving three cases concerning data security practices alleged to violate the Fair Credit Reporting Act, that it had "applied the standard that is consistent with its other data security cases – that of reasonable security. This reasonableness standard is flexible and recognizes that there is no such thing as perfect security.")

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 this proceeding.

Fourth, the Complaint alleges that the actual and potential data breaches it attributes to LabMD's data security practices caused or were likely to cause cognizable, "substantial injury" to consumers, including increased risks of "identity theft, medical identity theft," and "disclosure of sensitive private medical information." *See* Complaint, ¶ 12; *see also id.*, ¶¶ 11, 21-22. These allegations clearly refute LabMD's contentions that the Complaint contains "no allegations of monetary loss or other actual harm" nor "any actual, completed economic harms or threats to health or safety." Motion at 28-29. Moreover, occurrences of actual data security breaches or "actual, completed economic harms" (*id.* at 29) are not necessary to substantiate that the firm's data security activities caused or likely caused consumer injury, and thus constituted "unfair . . . acts or practices." *Accord Policy Statement on Unfairness*, 104 F.T.C. at 949 n.12 (act or practice may cause "substantial injury" if it causes a "small harm to a large number of people" or "raises a significant *risk* of concrete harm") (emphasis added); *accord Neovi*, 604 F.3d at 1157 (quoting *Am. Fin. Servs.*, 767 F.2d at 972).

B. Avoidability

The Complaint contains plausible allegations that these harms could not reasonably be avoided by consumers. Consumers allegedly did not have any "way of independently knowing about respondent's security failures," let alone taking any action to remedy them or avoid the resulting harm. Complaint, ¶ 12.

C. Countervailing Benefits to Consumers or Competition

Finally, the Complaint alleges that the alleged conduct did not even benefit LabMD, much less anyone else (*id.*, ¶ 20), and that LabMD could have remedied the risks of data breaches "at relatively low cost" (*id.*, ¶ 11). These allegations provide a plausible basis for finding that the harms to consumers were not outweighed by other benefits to consumers or competition. Again, Complaint Counsel will need to prove these allegations, and LabMD will have the opportunity to refute them, on the basis of factual evidence presented at the upcoming hearing.

* * * * *

For the reasons discussed above, we deny LabMD's Motion to Dismiss.

Accordingly,

IT IS ORDERED THAT Respondent LabMD, Inc.'s Motion to Dismiss Complaint with Prejudice **IS DENIED.**

By the Commission, Commissioner Brill recused.

Donald S. Clark
Secretary

SEAL:
ISSUED: January 16, 2014