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