No. 14-3514

In the United States Court of Appeals for the Third Circuit

FEDERAL TRADE COMMISSION

v.

WYNDHAM WORLDWIDE CORP., a Delaware corporation,
WYNDHAM HOTEL GROUP, LLC, a Delaware limited liability company,
WYNDHAM HOTELS & RESORTS, LLC, a Delaware limited liability company,
and WYNDHAM HOTEL MANAGEMENT, INC., a Delaware corporation

WYNDHAM HOTELS & RESORTS, LLC,

Appellant

On Appeal from the U.S. District Court for the District of New Jersey (Salas, J.)
Civil Action No. 2:13-cv-01887-ES-JAD

APPELLANT'S OPENING BRIEF AND JOINT APPENDIX VOL. 1, pp. JA1-55

Michael W. McConnell
STANFORD LAW SCHOOL
559 Nathan Abbott Way
Stanford, CA 94305
(650) 736-1326

Eugene F. Assaf, P.C.
Christopher Landau, P.C.
Susan M. Davies
K. Winn Allen
KIRKLAND & ELLIS LLP
655 Fifteenth St. N.W.
Washington, DC 20005
(202) 879-5000

Counsel for Appellant Wyndham Hotels & Resorts, LLC

Additional Counsel Listed on Inside Cover

October 6, 2014

Additional Counsel for
Appellant Wyndham Hotels & Resorts, LLC

Douglas H. Meal
David T. Cohen
ROPES & GRAY LLP
800 Boylston Street
Boston, MA 02199
(617) 951-7000

Jennifer A. Hradil
Justin T. Quinn
GIBBONS P.C.
One Gateway Center
Newark, NJ 07102
(973) 596-4500

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 and Third Circuit LAR 26.1, Appellant Wyndham Hotels & Resorts, LLC makes the following disclosure:

I. For non-governmental corporate parties please list all parent corporations:

Appellant Wyndham Hotels & Resorts, LLC is a wholly owned subsidiary of Wyndham Hotel Group, LLC, which in turn is a wholly owned subsidiary of Wyndham Worldwide Corporation.

II. For non-governmental corporate parties please list all publicly held companies that hold 10% or more of the party's stock:

Appellant Wyndham Hotels & Resorts, LLC is a wholly owned subsidiary of Wyndham Hotel Group, LLC, which in turn is a wholly owned subsidiary of Wyndham Worldwide Corporation, a publicly held company.

III. If there is a publicly held corporation which is not a party to the proceeding before this Court but which has as a financial interest in the outcome of the proceeding, please identify all such parties and specify the nature of the financial interest or interests:

None

IV. In all bankruptcy appeals counsel for the debtor or trustee of the bankruptcy estate must list: 1) the debtor, if not identified in the case caption; 2) the members of the creditors' committee or the top 20 unsecured creditors; and, 3) any entity not named in the caption which is an active participant in the bankruptcy proceeding. If the debtor or trustee is not participating in the appeal, this information must be provided by appellant.

N/A

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Rules

Other Authorities

INTRODUCTION

Hardly a day goes by now without revelations that some entity—whether a government agency, a leading academic institution, or a large corporation—has been "hacked," and its electronic data compromised. Cybersecurity—a word that did not even exist just a few years ago—is now a vital economic and national security concern, and a field of endeavor that has engaged many of the brightest minds in the Nation and around the world. Unfortunately, however, many other bright minds—often far away, in Russia or China—are just as keenly engaged in seeking to circumvent cybersecurity protections. Modern life thus entails a constant game of cat-and-mouse between cybersecurity professionals and sophisticated cyber-criminals. No entity or person is immune from the threat.

Appellant Wyndham Hotels & Resorts, LLC ("Wyndham") was among the victims. On three occasions between 2008 and 2010, sophisticated criminal hackers (apparently from Russia) gained unauthorized access into Wyndham's computer network as well as the computer networks of several Wyndham-branded hotels. By breaching the networks of the Wyndham-branded hotels, the attacks compromised

payment-card information that those hotels had collected from customers. Wyndham promptly reported these "hacking" incidents to law-enforcement authorities.

Instead of trying to develop national cybersecurity standards, or otherwise help Wyndham and other American businesses protect themselves from this ongoing threat, the Federal Government—through the Federal Trade Commission ("FTC")—responded by launching this lawsuit *against* Wyndham. According to the FTC, Wyndham engaged in "unfair ... acts or practices" in violation of the Federal Trade Commission Act, 15 U.S.C. § 45(a), by failing to take "reasonable and appropriate" measures to protect the data stolen by the criminal hackers (who have never been apprehended).

This lawsuit represents classic administrative overreaching. Until the decision below, no court in the history of American law had ever interpreted the FTC's authority over "unfair" business practices to encompass a company's efforts to secure its own computer networks. That is no surprise, as the FTC Act is not a federal cybersecurity statute; rather, it seeks to protect consumers from unscrupulous business practices. As a matter of law and common sense, a business

cannot be deemed to have engaged in an "unfair" practice where, as here, that business *itself* was the victim of criminal conduct by others. There is no allegation here (nor could there plausibly be) that Wyndham sought to take advantage of its customers, or had any incentive to tolerate or encourage the hackers' crimes. The word "unfair" may be broad, but it is not boundless. If that word is to have any meaning at all—and certainly to avoid serious constitutional concerns—it cannot be construed to apply here. It is implausible, to say the least, that Congress gave the FTC regulatory authority over a field as far-reaching and complex as cybersecurity by authorizing the agency to regulate "unfair" business practices.

And even assuming *arguendo* that the FTC had the statutory authority to interpret "unfair" business practices to encompass cybersecurity, the agency did not provide constitutionally adequate notice of what cybersecurity practices violate the statute. The rule of law depends on providing citizens with fair notice of what the law requires and proscribes. And the point here is simple: the FTC has never identified *any* standard, or otherwise provided any meaningful guidance, regarding what cybersecurity measures are "reasonable and

appropriate." In the absence of such guidance, businesses cannot conform their conduct to the law, and are subject to enforcement at the FTC's whim—the very antithesis of the rule of law. The Commission has simply anointed itself a roving cybersecurity prosecutor—but, unlike other prosecutors, one that seeks to define the offense and to do so after the fact. Precisely because cybersecurity affects everyone—including the FTC (which itself was recently victimized by cyberhackers)—this *ad hoc* and *post hoc* prosecutorial regime is neither lawful nor desirable.

What is particularly anomalous here is that the FTC is seeking to prosecute a victim of cybercrime, like Wyndham, where *no* consumer suffered a "substantial" injury that was not "avoidable," and thus the FTC cannot establish these statutory requirements for an "unfair" business practice. The FTC's complaint certainly does not plead any *facts* showing that any consumers sustained substantial and non-avoidable injuries as a result of the cybercriminals' attacks on Wyndham. That factual omission is no oversight, as any consumer could avoid fraudulent charges by simply notifying his or her payment-card company. Thus, above and beyond the far-reaching statutory and

constitutional issues presented by this case, the district court should have dismissed the "unfair" practice count on the familiar ground that the complaint fails to satisfy federal pleading standards.

Let there be no mistake: cybersecurity is among the most significant public policy issues of our times. And precisely because the issue is so important, it must be handled right. The President, Congress, and private stakeholders are engaged in an ongoing dialogue on how to address the emerging phenomenon of cybercrime, including how best to allocate costs and responsibilities and how to weigh the complex interactions of various technologies. However these issues are ultimately resolved, one thing is clear: the FTC is not empowered to prosecute businesses for allegedly failing to adopt "reasonable and appropriate" cybersecurity practices, particularly when, as discussed in this brief, (1) the FTC has no statutory authority to regulate cybersecurity, (2) the FTC has failed to provide any fair notice as to what constitutes "reasonable and appropriate" cybersecurity, and (3) the FTC cannot plead facts to establish substantial or non-avoidable injury to consumers.

Accordingly, this Court should reverse the order under review and direct the district court to enter judgment in Wyndham's favor on Count II of the FTC's amended complaint.

STATEMENT OF JURISDICTION

The district court has subject-matter jurisdiction over this case pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345. That court denied Wyndham's motion to dismiss the FTC's complaint on April 7, 2014, JA1-43, and certified that order for interlocutory review under 28 U.S.C. § 1292(b) on June 23, 2014, JA44-53.

This Court has jurisdiction over this interlocutory appeal because it granted Wyndham's petition for leave to appeal under 28 U.S.C. § 1292(b) on July 29, 2014. *See* JA54-55.

STATEMENT OF THE ISSUES[1]

1. Whether an alleged failure to provide "reasonable and appropriate" cybersecurity is an "unfair" business practice under Section 5 of the FTC Act. *See* JA3; JA8-16; Mot. to Dismiss 7-14 (4/26/13) [Dist. Ct. Dkt. No. 91-1].

2. Whether the FTC has provided constitutionally adequate notice of what are "reasonable and appropriate" cybersecurity practices. *See* JA3; JA16-26; Mot. to Dismiss 14-19.

3. Whether the FTC has pleaded sufficient facts to state a plausible claim of "substantial" injury to consumers that is not "avoidable" by consumers. *See* JA3; JA26-34; Mot. to Dismiss 19-23.

---

[1] The district court's order granting Wyndham's motion to certify this appeal for interlocutory review under 28 U.S.C. § 1292(b) framed the questions somewhat differently. *See* JA52-53. That difference, however, is immaterial. Certification under § 1292(b) "applies to the *order* certified to the court of appeals, and is not tied to the particular *question* formulated by the district court." *Yamaha Motor Corp., USA v. Calhoun*, 516 U.S. 199, 205 (1996) (emphasis modified). Accordingly, "the appellate court may address any issue fairly included within the certified order," regardless of how the district court framed the issues. *Id.* All three of the issues presented here are expressly addressed in the certified order.

STATEMENT OF RELATED CASES

This case has never previously been before this Court. Proceedings in the district court remain ongoing while this Court considers this interlocutory appeal. *See* No. 2:13-cv-01887 (D.N.J.).

STATEMENT OF THE CASE AND FACTS

Because this appeal arises in the context of a motion to dismiss on the pleadings, this Court must accept the truth of the well-pleaded factual allegations in the complaint. *See*, *e.g.*, *Bell v. Cheswick Generating Station*, 734 F.3d 188, 193 n.5 (3d Cir. 2013). Although Wyndham by no means concedes the truth of the complaint's factual allegations, the key point here is that Wyndham is entitled to judgment as a matter of law on the "unfairness" count of the complaint regardless of the truth of those allegations.

A. Background

Wyndham is a hospitality company that provides services to over 100 hotels operating under the Wyndham brand name. Am. Compl. [Dist. Ct. Dkt. No. 28] ¶¶ 9, 13, JA59-61. With a few exceptions, each of those hotels is independently owned by a third party, and the independent owners are authorized to use the Wyndham brand name pursuant to franchise agreements. *See id.* As part of that franchise

relationship, Wyndham operates and maintains a computer network to provide certain information technology services to the Wyndham-branded hotels. *Id.* ¶ 16, JA62. Each Wyndham-branded hotel also operates and maintains its own computer network separate from, but usually linked to, the Wyndham network. *Id.* ¶ 15, JA62.

On three occasions from 2008 to 2010, sophisticated criminal hackers gained unauthorized access into the Wyndham computer network and the computer networks of several Wyndham-branded hotels. *Id.* ¶ 25, JA67-68. On each occasion, the hackers were able "to access personal information stored on the Wyndham-branded hotels' property management system servers, including customers' payment card account numbers, expiration dates, and security codes." *Id.* The hackers exported the data "to a domain registered in Russia." *Id.* ¶¶ 2, 32, 40, JA57, 70, 73.

In the aftermath of these cyberattacks, the FTC launched an investigation into Wyndham's data-security practices. Over the course of that two-year investigation, Wyndham produced over one million pages of documents, answered over fifty written interrogatories, and gave seven in-person presentations.

B. Proceedings Below

On June 26, 2012, the Commission filed this lawsuit against Wyndham and three corporate affiliates in the U.S. District Court for the District of Arizona. *See* Compl. (6/26/12) [Dist. Ct. Dkt. No. 1]. The complaint, as amended, alleges that defendants "have failed to employ reasonable and appropriate measures to protect personal information against unauthorized access." Am. Compl. (8/9/12) [Dist. Ct. Dkt. No. 28] ¶ 47, JA74; *see also id.* ¶ 1, JA57 (alleging that defendants "fail[ed] to maintain reasonable and appropriate data security for consumers' sensitive personal information"). As relevant here, Count II of the complaint alleges that these actions "constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n)." *Id.* ¶ 49, JA74.[2] As relief, the FTC requests (1) "a permanent injunction to prevent future violations of the FTC Act by Defendants," (2) "such relief as the Court finds necessary to redress injury to consumers

[2] Count I of the complaint alleges that defendants also engaged in "deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a)," on the theory that "in connection with the advertising, marketing, promotion, offering for sale, or sale of hotel services, Defendants have represented, directly or indirectly, expressly or by implication, that they had implemented reasonable and appropriate measures to protect personal information against unauthorized access." Am. Compl. ¶¶ 44, 46, JA73-74.

resulting from Defendants' violations of the FTC Act, including but not limited to, rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies," and (3) an award of "the costs of bringing this action." *Id.*, Prayer for Relief, JA75-76.

Defendants promptly moved to transfer the case to New Jersey, where they are headquartered. Over the FTC's objection, the Arizona district court (Rosenblatt, J.) granted the motion. *See* Order (3/25/13) [Dist. Ct. Dkt. No. 77].

Wyndham thereafter moved to dismiss Count II of the complaint—the "unfair" practices count—as a matter of law on the grounds that (1) the FTC lacks the authority to regulate cybersecurity under Section 5 of the FTC Act, (2) even if the FTC had such authority, it failed to provide constitutionally adequate notice of what cybersecurity practices were required, and (3) the FTC's complaint failed to plead facts sufficient to establish a plausible violation of the Act. *See* Mot. to Dismiss (4/26/13) [Dist. Ct. Dkt. No. 91-1].[3] After

[3] Concurrent with Wyndham's motion to dismiss, the three other defendants (Wyndham Worldwide Corporation, Wyndham Hotel Group, LLC, and Wyndham Hotel Management, Inc.) filed a separate motion to

hearing argument on the matter, *see* Tr. (11/7/13) [Dist. Ct. Dkt. No. 139], JA79-264, the district court (Salas, J.) denied the motion, *see* Opinion (4/7/14) [Dist. Ct. Dkt. No. 181], JA2-43; Order (4/7/14) [Dist. Ct. Dkt. No. 182], JA1.

In denying the motion, the district court repeatedly characterized Wyndham's position as seeking to "*carve out* a data-security *exception* to the FTC's authority." JA7 (emphasis added); *see also* JA11 (same); JA15 (same); JA16 (same). A request to "carve out" an "exception" to agency authority, of course, presupposes that the agency had such authority in the first place. But Wyndham's position is just the opposite: that Section 5 of the FTC Act never gave the FTC the authority to regulate cybersecurity as an "unfair" business practice at all. The district court simply dodged that bedrock issue by insisting

---

dismiss "to address certain elements of the FTC's allegations that pertain only to them"—the FTC's attempt "to hold those separate corporate entities derivatively liable for the allegedly unlawful conduct that was undertaken by [Wyndham] alone." Mot. to Dismiss (4/26/13) [Dist. Ct. Dkt. No. 92-1]. The district court denied that motion on the same day that it granted Wyndham's motion to certify this appeal for interlocutory review. *See* Opinion (6/23/14) [Dist. Ct. Dkt. No. 201]; Order (6/23/14) [Dist. Ct. Dkt. No. 202]. Accordingly, the order denying the other defendants' motion to dismiss is not within the scope of this interlocutory appeal.

that Wyndham had failed to demonstrate that Congress had "carved out" a cybersecurity "exception" to the FTC's authority. And the court similarly dodged Wyndham's fair-notice argument by insisting that "the FTC need not formally issue regulations ... before bringing its unfairness claim," JA3—thereby again rejecting an argument that Wyndham had never made.[4]

The district court, however, granted Wyndham's subsequent motion to certify the order for interlocutory appeal under 28 U.S.C. § 1292(b). *See* Order (6/23/14) [Dist. Ct. Dkt. No. 203], JA44-53. In the certification order, the court held that "reasonable jurists may differ over the Court's resolution" of the issues decided in the order denying the motion to dismiss. JA49. Specifically, the court opined that the "statutory authority and fair-notice challenges confront this Court with novel, complex statutory interpretation issues that give rise to a

[4] The district court also denied Wyndham's motion to dismiss the FTC's complaint insofar as it related to Count I, the "deception" count, which charges Wyndham with making false or misleading representations about its cybersecurity practices. *See* JA34-43. Although Wyndham also disagrees with the district court's order on this issue, Count I does not present any overriding question of statutory or constitutional interpretation, and hence Wyndham did not seek interlocutory review on that issue.

substantial ground for difference of opinion." *Id.* The court also acknowledged "the absence of precedent directly addressing the pure questions of law" at stake here. JA52.

This Court subsequently granted Wyndham's petition for leave to appeal. *See* Order (7/29/14), JA54-55. Meanwhile, proceedings in the district court continue apace. To date, the FTC has served 111 document requests, sought leave to take the depositions of 35 fact witnesses, *see* Proposed Joint Discovery Plan at 8 (12/18/13) [Dist. Ct. Dkt. No. 143-1], and sought a five-month extension of the fact-discovery period, *see* K. Moriarty Letter to the Court (7/14/14) [Dist. Ct. Dkt. No. 211]. The district court limited the FTC to 100 hours of depositions, *see* Pretrial Scheduling Order (1/7/14) [Dist. Ct. Dkt. No. 148], and extended the fact-discovery period by approximately three months, *see* Amended Scheduling Order (8/13/14) [Dist. Ct. Dkt. No. 224]. Fact discovery is now scheduled to close in December 2014, and expert discovery is scheduled to begin shortly thereafter. *Id.*

SUMMARY OF ARGUMENT

This Court should reverse the district court's order denying Wyndham's motion to dismiss Count II of the Amended Complaint—the "unfair" practices count—for three separate reasons.

First, the FTC's authority to regulate "unfair" business practices does not extend, as a matter of law, to regulating a company's cybersecurity practices. A business treats consumers unfairly when it seeks to take advantage of them, or otherwise injures them through unscrupulous or unethical behavior. As a matter of law and logic, a business does not treat its customers unfairly when the business *itself* is victimized by criminals, and the business' customers are thereby injured (if at all) only derivatively. The FTC's authority to regulate "unfair" business practices thus does not encompass the authority to regulate the practices by which a business protects itself (and hence, derivatively, its customers) from criminals. If Congress had intended to give the FTC vast powers over cybersecurity (or other forms of business security), it could and would have done so much more clearly than allowing the Commission to regulate "unfair" business practices. And

because the statutory term "unfair" cannot be stretched so far, the FTC is not entitled to any deference on this score.

Second, the FTC's attempt to exercise its supposed cybersecurity authority here does not comport with basic norms of fair notice protected by the Due Process Clause. The FTC alleges that Wyndham's cybersecurity practices are not "reasonable or appropriate." But the FTC has never provided any notice as to what "reasonable or appropriate" cybersecurity practices might be, either for Wyndham or for any other business of any size. In essence, the Commission has adopted a "we know it when we see it" approach that leaves every business in the land vulnerable to selective enforcement. That approach is fundamentally inconsistent with the rule of law, which depends upon providing fair notice of what the law requires and proscribes.

And *third*, above and beyond those far-reaching statutory and constitutional issues, the FTC's complaint fails to plead facts to state a plausible claim of a violation of the statute. Among other things, an "unfair" business practice must cause "substantial" injury to consumers that is not "avoidable" by consumers. The complaint here fails to plead

any facts showing that consumers have sustained substantial and non-avoidable injuries. That is not surprising, as any consumer could avoid any fraudulent charges by simply notifying his or her payment-card company.

STANDARD OF REVIEW

This Court reviews *de novo* a district court's ruling on a motion to dismiss for failure to state a claim. *See, e.g.*, *McTernan v. City of York*, 577 F.3d 521, 526, 530-31 (3d Cir. 2009) (citing *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), and *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007)). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 570). "Factual allegations must be enough to raise a right to relief above the speculative level," *Twombly*, 550 U.S. at 555, and a complaint must plead specific facts that raise "more than a sheer possibility that a defendant has acted unlawfully," *Iqbal*, 556 U.S. at 678. A court need not, and may not, accept legal conclusions packaged as factual allegations. *See*, *e.g.*, *Iqbal*, 556 U.S. at 678-79; *Twombly*, 550 U.S. at 555-56.

ARGUMENT

I. An Alleged Failure To Provide "Reasonable And Appropriate" Cybersecurity Is Not An "Unfair" Business Practice Under Section 5 Of The FTC Act.

The district court erred, first and foremost, by assuming the answer to the core question presented here: whether the FTC's authority over "unfair" business practices, 15 U.S.C. § 45(a), encompasses a company's alleged failure to adopt "reasonable and appropriate" measures to protect its computer networks from hackers. Administrative agencies are creatures of statute, and thus "an agency literally has no power to act ... unless and until Congress confers power upon it." *Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986). The district court missed this fundamental point by holding that Wyndham had failed to demonstrate the need to "*carve out* a data-security *exception* to the FTC's authority." JA7 (emphasis added); *see also* JA11 (same); JA15 (same); JA16 (same). This case is not about "a data-security *exception* to the FTC's authority"; it is about the scope of the FTC's authority to regulate "unfair" business practices in the first place.

As a matter of ordinary English, an "unfair" business practice is one "marked by injustice, partiality, or deception," *i.e.*, one that is "not

equitable." *Webster's Ninth New Collegiate Dictionary* (1988); *see also LeBlanc v. Unifund CCR Partners*, 601 F.3d 1185, 1200 (11th Cir. 2010) (*per curiam*) ("The plain meaning of 'unfair' is 'marked by injustice, partiality, or deception.'") (internal quotation omitted). There is no reason to think that the meaning of the word "unfair" in the FTC Act differs from its meaning in ordinary English. Although it may be impossible "to attempt a comprehensive definition of the unfair methods which are banned" by the Act, *FTC v. R.F. Keppel & Bro., Inc.*, 291 U.S. 304, 314 (1934), that does not mean that the scope of the word "unfair" is boundless, *see, e.g.*, *Scientific Mfg. Co. v. FTC*, 124 F.2d 640, 643-44 (3d Cir. 1941). It is the courts' responsibility to enforce the boundaries of that statutory term. "[T]he Commission is hardly free to write its own law of consumer protection," and "the judiciary remains the final authority with respect to questions of statutory construction and must reject administrative agency actions which exceed the agency's statutory mandate or frustrate congressional intent." *American Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 968 (D.C. Cir. 1985) (internal quotation omitted). A court owes an administrative agency no deference where, as here, the court is called upon to enforce the

boundaries of Congress' statutory delegation of authority to the agency in the first place. *See, e.g.*, *Chevron USA, Inc. v. NRDC, Inc.*, 467 U.S. 837, 842-43 (1984); *see also National Credit Union Admin. v. First Nat'l Bank & Trust Co.*, 522 U.S. 479, 499-500 (1998); *Prestol-Espinal v. Attorney General of U.S.*, 653 F.3d 213, 215 (3d Cir. 2011).

The key point here is that the term "unfair" in Section 5 of the FTC Act cannot be stretched to encompass a company's alleged failure to adopt "reasonable and appropriate" measures to protect its computer networks from hackers. That provision, as relevant here, governs a business' acts or practices vis-à-vis consumers. *See, e.g.*, *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 244 (1972); *cf.* 15 U.S.C. § 45(n).[5] A business treats consumers "unfairly" when it seeks to take advantage of them, or otherwise injures them through unscrupulous or unethical

[5] As originally enacted in 1914, the FTC Act proscribed only "unfair methods of competition." Pub. L. No. 203, 38 Stat. 719 (1914). The statute was amended in 1938 to extend the statute's scope to "unfair or deceptive acts or practices." *See* Pub. L. No. 447, 52 Stat. 111 (1938). The legislative history of the 1938 amendment states that Congress sought to "make[] the consumer, who may be injured by an unfair trade practice, of equal concern, before the law, with the merchant or manufacturer injured by the unfair methods of a dishonest competitor." H.R. Rep. No. 75-1613, at 3 (1937); *see also* S. Rep. No. 74-1705, at 2-3 (1936).

behavior. *See, e.g.*, *R.F. Keppel*, 291 U.S. at 313. As a matter of law and logic, a business does not treat its customers in an "unfair" manner when the business *itself* is victimized by criminals. Regardless of whether the business could or should have done more to thwart the criminals, it is not acting "unfairly" to its customers under these circumstances: it has not sought to take advantage of them, and it certainly has no incentive to tolerate or encourage crimes against itself. After all, any injury to consumers is derivative of the injury to the business itself from the crime.

The Commission seeks to sidestep this point by referring to Section 5(n) of the Act, 15 U.S.C. § 45(n). That approach is not only misguided, but ironic. Congress added that provision to the statute in 1994 (after substantial controversy about several of the Commission's regulatory efforts) to *limit* the agency's discretion to declare business acts or practices "unfair." *See* FTC Amendments Act of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695 (codified at 15 U.S.C. § 45(n)). Section 5(n) specifies that "[t]he Commission shall have *no* authority ... to declare unlawful an act or practice on the grounds that such act or practice is unfair *unless* the act or practice causes or is likely to cause

substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n) (emphasis added). By its plain terms, that provision *adds* requirements to the "unfairness" determination; it does not *subtract* anything. Thus, in order for an act or practice to be "unfair" under Section 5(a), it is *necessary* but not *sufficient* that it meet the criteria of Section 5(n). An act or practice that is not otherwise unfair does not become "unfair" within the meaning of the statute just because it satisfies Section 5(n).

The district court's decision suggests no meaningful limiting principle on the scope of the statutory word "unfair." If the FTC's regulatory jurisdiction extends to any and all business acts or practices that may in some way result in injury to consumers—even if those acts or practices do not involve any element of unfairness to the consumers—then the FTC's regulatory jurisdiction over American business is boundless. Under this view, the FTC could regulate not just data security, but any act or practice by any consumer business. Certainly, cybersecurity is no different in kind from physical security, so the FTC's assertion of regulatory authority here, if upheld, would

logically mean that the FTC has authority to regulate the locks on hotel room doors or to require every store in the land to post an armed guard at the door. But none of this, of course, has anything to do with "unfair" trade practices under the FTC Act. Just because cybersecurity is an important issue does not mean that the FTC has the statutory authority to regulate it. "Regardless of how serious the problem an administrative agency seeks to address, ... it may not exercise its authority in a manner that is inconsistent with the administrative structure that Congress enacted into law." *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 125 (2000) (internal quotations omitted).

It is far-fetched, to say the least, to suppose that Congress gave the FTC not only the authority to protect consumers from "unfair" business practices but also a roving commission to safeguard consumer information. As the Supreme Court recently reiterated, courts should meet an agency's assertion of such far-reaching authority "with a measure of skepticism," particularly where, as here, the agency "claims to discover in a long-extant statute an unheralded power to regulate a significant portion of the American economy." *Utility Air Regulatory Grp. v. EPA*, 134 S. Ct. 2427, 2444 (2014) (internal quotation omitted).

That skepticism is warranted, the Court explained, because Congress will ordinarily "speak clearly if it wishes to assign to an agency decisions of vast economic and political significance"—decisions such as what are "reasonable and appropriate" cybersecurity practices in an age in which information technology pervades American businesses of all sizes and in all industries. *Id.*

Indeed, in recent years, Congress has enacted statutes that specifically authorize the FTC to establish federal cybersecurity standards in certain narrow and defined sectors of the economy. For instance, the Fair Credit Reporting Act ("FCRA") imposes requirements for the collection, disclosure, and disposal of data collected by consumer reporting agencies, and directs the FTC and other federal agencies to develop additional regulations for financial institutions to protect sensitive consumer data and reduce the incidence of identity theft. *See* Pub. L. No. 108-159, § 216(a), 117 Stat. 1952, 1985 (2003) (codified as amended at 15 U.S.C. § 1681w). Similarly, the Gramm-Leach-Bliley Act ("GLBA") directs the FTC and federal banking regulators to "establish appropriate standards" for "administrative, technical, and physical safeguards" that (1) "insure the security and confidentiality of

customer records and information" held by certain financial institutions; (2) "protect against any anticipated threats or hazards to the security or integrity of such records"; and (3) "protect against unauthorized access to or use of such records or information." Pub. L. No. 106-102, § 501(b), 113 Stat. 1338, 1346-47 (1999) (codified as amended at 15 U.S.C. § 6801(b)).[6]

These tailored grants of substantive authority to the FTC in the cybersecurity field would be inexplicable if the Commission already had general substantive authority over this field. *See*, *e.g.*, *Brown & Williamson*, 529 U.S. at 143 ("The 'classic judicial task of reconciling many laws enacted over time, and getting them to 'make sense' in combination, necessarily assumes that the implications of a statute may be altered by the implications of a later statute.' This is particularly so

[6] In addition, Congress has enacted several other statutes to address cybersecurity concerns in discrete and tailored segments of the national economy. *See, e.g.*, Children's Online Privacy Protection Act of 1998 ("COPPA"), Pub. L. No. 105-277, §§ 1303-06, 112 Stat. 2681, 2730-35 (codified as amended at 15 U.S.C. §§ 6502-05); Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, § 262(a), 110 Stat. 1936, 2025-26 (codified as amended at 42 U.S.C. § 1320d-2(d)); Health Information Technology for Economic and Clinical Health Act ("HITECH"), Pub. L. No. 111-5, § 13402(h), 123 Stat. 115, 262-63 (codified as amended at 42 U.S.C. § 17932(h)).

where the scope of the earlier statute is broad but the subsequent statutes more specifically address the topic at hand.'") (quoting *United States v. Fausto*, 484 U.S. 439, 453 (1988)); *United States v. Estate of Romani*, 523 U.S. 517, 530-31 (1998) ("[A] specific policy embodied in a later federal statute should control our construction of the [earlier] statute, even though it ha[s] not been expressly amended."); *West Va. Univ. Hosps., Inc. v. Casey*, 499 U.S. 83, 101 (1991) ("[I]t is our role to make sense rather than nonsense out of the *corpus juris*.").

The district court, however, declared that "subsequent data-security legislation seems to complement—*not preclude*—the FTC's authority." JA12 (emphasis in original). But these recent statutes cannot be dismissed as simply interstitial or supplemental; to the contrary, they presuppose the absence, not the presence, of pre-existing substantive authority in this area. *See* 15 U.S.C. § 1681m(e)(1)(A) (FCRA provision directing the FTC and other federal agencies to "establish and maintain guidelines for use by each financial institution and each creditor regarding identity theft with respect to accountholders"); *id.* § 1681s(a)(1) (FCRA provision authorizing the FTC "to enforce compliance with the requirements imposed by" that statute);

id. § 6804(a)(1)(C) (GLBA provision granting the FTC authority to "prescribe such regulations as may be necessary to carry out the purposes" of the statute, including its data-security provisions); *id.* § 6805(a)(7) (GLBA provision directing the FTC to enforce that statute "and the regulations prescribed thereunder"). Congress knows how to target cybersecurity when it wishes to do so, and Congress did not do so in the "unfair" practices provision of the FTC Act. *See, e.g.*, *Brown & Williamson*, 529 U.S. at 160.

Indeed, the legislative history of the FCRA and GLBA refutes any suggestion that these statutes were enacted merely to supplement some pre-existing general authority over cybersecurity. Each statute was enacted in response to congressional concerns over the collection and misuse of sensitive consumer data. *See, e.g.*, H.R. Rep. No. 108-396, at 65-66 (2003) (Conf. Rep.) (explaining that the 2003 amendments to the FCRA, which granted the FTC narrow data-security authority over disposal of certain information derived from consumer credit reports, were enacted in response to "the explosive growth of a new crime—identity theft"); *see also* H.R. Rep. No. 106-74, pt. 3, at 117-19 (1999) (committee report on the GLBA). The whole reason for enacting these

statutes was that Congress believed that data security *was not covered by existing statutory provisions*, including Section 5 of the FTC Act. It would certainly have been strange for Congress to enact these carefully tailored statutes to give the FTC a scalpel in the emerging cybersecurity field if the Commission already wielded a meat-axe.

In addition, 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. For over a decade, the FTC has lobbied in favor of legislation that would establish substantive federal cybersecurity standards for American business, and give the FTC the authority to enforce those standards. *See, e.g.*, *Consumer Data Protection: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong., 2011 WL 2358081, at 6 (June 15, 2011) (statement of Edith Ramirez, Commissioner, FTC); *Data Theft Issues: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong., 2011 WL 1971214, at 7 (May 4, 2011) (statement of David C. Vladeck, Director, FTC Bureau of Consumer Protection); FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to*

Congress, at 36-37 (May 2000), *available at* http://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission; *Privacy in Cyberspace: Hearing Before the Subcomm. on Telecomms., Trade & Consumer Protection of the H. Comm. on Commerce*, 105th Cong., 1998 WL 546441, at 9-10 & n.23 (July 21, 1998) (statement of Robert Pitofsky, Chairman, FTC); *see also* Michael D. Scott, *The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has The Commission Gone Too Far?*, 60 Admin. L. Rev. 127, 130-31 (2008).

Indeed, consistent with these requests for authority, Congress has considered a variety of cybersecurity bills—including one that would have required the Secretary of Homeland Security to "identify or develop, on a sector-by-sector basis, risk-based cybersecurity performance requirements," S. 2105, 112th Cong. § 104 (2012), and another that would have required businesses to establish "administrative, technical, or physical safeguards identified by the Federal Trade Commission in a rulemaking process" to protect consumer data, S. 1151, 112th Cong. § 302 (2011). After much debate, however, none of these bills passed. Thus, in February 2013, the

President issued an Executive Order and a Presidential Policy Directive on cybersecurity issues, which require the development of minimum data-security standards for businesses operating critical-infrastructure systems or assets. *See* Exec. Order. No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013); Presidential Policy Directive PPD-21 (Feb. 12, 2013). Needless to say, this activity would make no sense if the FTC already had sweeping authority to regulate cybersecurity as an "unfair" business practice under Section 5 of the FTC Act.

Moreover, the intense legislative debate surrounding these and numerous other cybersecurity bills, *e.g.*, S. 1976, 113th Cong. (2014); S. 1927, 113th Cong. (2014); S. 3414, 112th Cong. (2012), demonstrates the importance and sensitivity of establishing federal cybersecurity standards. Courts must "be guided to a degree by common sense as to the manner in which Congress is likely to delegate a policy decision of such economic and political magnitude to an administrative agency." *Brown & Williamson*, 529 U.S. at 133. In light of the important economic and political considerations involved in establishing federal cybersecurity standards for the private sector, and the intense political debate that has surrounded efforts to enact such standards, it defies

"common sense" to suppose that Congress delegated that responsibility to the FTC through a statute that does nothing more than proscribe "unfair" business practices. *See id.* at 160 ("Congress could not have intended to delegate a decision of such economic and political significance to an agency in so cryptic a fashion."); *see also Utility Air Regulatory Grp.*, 134 S. Ct. at 2444 (explaining that EPA's claimed authority to regulate certain greenhouse gas emissions amounts to "extravagant statutory power over the national economy" that "falls comfortably within the class of authorizations that we have been reluctant to read into ambiguous statutory text"); *Gonzales v. Oregon*, 546 U.S. 243, 267 (2006) (rejecting the "idea that Congress gave the Attorney General such broad and unusual authority through an implicit delegation"); *Whitman v. American Trucking Ass'ns, Inc.*, 531 U.S. 457, 468 (2001) ("[W]e find it implausible that Congress would give to the EPA through ... modest words the power to determine whether implementation costs should moderate national air quality standards."); *MCI Telecomm. Corp. v. AT&T Co.*, 512 U.S. 218, 229, 231 (1994) (holding that the FCC's power to "modify" requirements in the

communications laws does not include the power to make "radical or fundamental" changes to regulatory requirements).

The district court below thus missed the point by asserting that "the FTC's unfairness authority over data security can coexist with the existing data-security regulatory scheme." JA13. The issue here is not whether such authority *can* coexist, but whether Congress intended for such coexistence. The subsequent legislative activity only confirms that the statutory grant of authority over "unfair" business practices does not extend to cybersecurity measures in the first place. To conclude that the FTC has the authority to regulate cybersecurity would require not only an implausible interpretation of "unfairness"—a concept central to the FTC Act's entire regulatory scheme—but also ignore the plain implication of Congress' subsequent cybersecurity-specific legislation. *See Brown & Williamson*, 529 U.S. at 159-60.

Finally, even if it were a close question whether the FTC's authority to regulate "unfair" trade practices encompasses the authority to regulate cybersecurity, the doctrine of constitutional avoidance would compel a negative answer. That doctrine requires courts, when choosing between competing interpretations of a statute, to choose the

interpretation that would avoid a serious constitutional question. *See*, *e.g.*, *Zadvydas v. Davis*, 533 U.S. 678, 689 (2001) ("'[I]t is a cardinal principle' of statutory interpretation ... that when an Act of Congress raises 'a serious doubt' as to its constitutionality, 'this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided.'") (quoting *Crowell v. Benson*, 285 U.S. 22, 62 (1932)); *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Building & Constr. Trades Council*, 485 U.S. 568, 575 (1988) ("[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress."). And this doctrine provides yet another basis for rejecting an administrative agency's request for judicial deference: courts need not, and may not, defer to agency interpretations of a statute that raise serious constitutional questions. *See, e.g.*, *Solid Waste Agency of N. Cook Cnty. v. U.S. Army Corps of Eng'rs*, 531 U.S. 159, 174 (2001); *Scientific Mfg.*, 124 F.2d at 644 (rejecting FTC interpretation of its Section 5 authority over "unfair" business practices that raised serious First Amendment question). Here, the FTC's

proffered interpretation of the statute raises a serious non-delegation question.

The non-delegation doctrine recognizes that the Constitution gives Congress the power to legislate, and Congress may not delegate that power to administrative agencies through standardless delegations of authority. *See, e.g.*, *Mistretta v. United States*, 488 U.S. 361, 371-79 (1989). If the power to regulate "unfair" business practices extends to the power to regulate cybersecurity, then the term "unfair" is effectively boundless, and Congress has unconstitutionally delegated legislative power to the FTC. The interpretation proposed here, in contrast, provides an "intelligible principle" to narrow the agency's discretion and thus avoids the serious constitutional problem posed by the FTC's interpretation. "A construction of the statute that avoids [an] open-ended grant should certainly be favored." *Industrial Union Dep't v. American Petroleum Inst.*, 448 U.S. 607, 646 (1980) (plurality opinion); *see also National Cable Television Ass'n, Inc. v. United States*, 415 U.S. 336, 342 (1974) (construing statute to avoid non-delegation question); *cf. Mistretta*, 488 U.S. at 373 n.7 ("In recent years, our application of the nondelegation doctrine principally has been limited to the

interpretation of statutory texts, and, more particularly, to giving narrow constructions to statutory delegations that might otherwise be thought to be unconstitutional."). Accordingly, this Court should hold that the FTC's authority to regulate "unfair" business practices does not encompass the authority to regulate cybersecurity.

II. The FTC Has Not Provided Constitutionally Adequate Notice Of What Are "Reasonable And Appropriate" Cybersecurity Practices.

The district court also erred by refusing to dismiss the FTC's complaint on constitutional fair-notice grounds. *See* JA16-26. It is a "fundamental principle in our legal system that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012); *see also PMD Produce Brokerage Corp. v. USDA*, 234 F.3d 48, 52 (D.C. Cir. 2000); *General Elec. Co. v. EPA*, 53 F.3d 1324, 1328-29 (D.C. Cir. 1995). Only where "a regulated party acting in good faith would be able to identify, with 'ascertainable certainty,' the standards with which the agency expects parties to conform" has an agency provided fair notice of the law. *General Elec.*, 53 F.3d at 1329 (internal quotation omitted). "This requirement of clarity in regulations is essential to the

protections provided by the Due Process Clause of the Fifth Amendment." *Fox*, 132 S. Ct. at 2317.

The complaint in this case charges Wyndham with violating the law by failing to adopt "reasonable and appropriate" cybersecurity practices. *See*, *e.g.*, Am. Compl. ¶¶ 1, 47, JA57, 74. But the FTC has never provided any guidance as to what cybersecurity practices are "reasonable and appropriate" in an era in which cybersecurity breaches are, unfortunately, a daily occurrence. *See* Verizon Enterprise Solutions, *2014 Data Breach Investigations Report* at 2, *available at http://www.verizonenterprise.com/DBIR/2014* (identifying, in 2013 alone, 63,437 "confirmed security incidents" that resulted in 1,367 "confirmed data breaches"). Thus, regulated entities like Wyndham had (and have) no way of conforming their conduct to the law, and the statute is a dragnet for the FTC to hold virtually any business in the land liable for violating an unknown (and unknowable) standard. Because that violates due process, the case should have been dismissed on this ground too. *See, e.g.*, *Fox*, 132 S. Ct. at 2317-20 (FCC could not find that companies violated the law, or fine them, when they lacked fair notice that their actions could violate the law); *PMD*, 234 F.3d at 52

(USDA could not sanction company without providing fair notice of its rules); *General Elec.*, 53 F.3d at 1328-34 (EPA could not impose fine on company without providing fair notice of its regulations).

In particular, the FTC has provided no guidance on what cybersecurity practices businesses must adopt (or avoid) to comply with the law. For instance, the Commission has provided *no* guidance as to (1) what firewall configurations a business must employ, (2) what types of MAC or IP address authentication are necessary, (3) what encryption techniques must be used to secure consumer data, or (4) what password requirements a business must impose on its employees. Yet the FTC alleged that Wyndham's data security was deficient in each of those four areas. *See, e.g.*, Am. Compl. ¶¶ 24(a), (b), (f), (j), JA65-67.

The FTC's failure to provide fair notice is no mere oversight. Rather, as one Commissioner explained earlier this year, the Commission has *deliberately* chosen an enforcement regime that is "*ex post* rather than *ex ante*" and "enforcement-centric rather than rulemaking-centric." Maureen K. Ohlhausen, *The Procrustean Problem with Prescriptive Regulation*, Remarks at the Free State Foundation Telecom Conference at 11 (Mar. 18, 2014) [hereinafter Ohlhausen, *The*

Procrustean Problem], *available at* http://www.ftc.gov/system/files/documents/public_statements/291361/140318fsf.pdf. The Commission has eschewed the "prescriptive *ex ante*" approach taken by other agencies, including the Federal Communications Commission, on the ground that such an approach is "very time consuming" and "not well suited to regulating the rapidly evolving Internet." *Id.* at 7. As another Commissioner recently put it, "[r]eflexive resistance to the imposition of any meaningful limits on the Commission from those who envision an agency with unbounded discretion is predictable." Joshua D. Wright *et al.*, *Defining Section 5 of the FTC Act: The Failure of the Common Law Method and the Case for Formal Agency Guidelines*, 21 Geo. Mason L. Rev. 1289, 1293 (2014).

The district court below framed the fair-notice issue here as whether "the FTC must formally promulgate regulations before bringing its unfairness claim." JA3; *see also* JA19 ("[T]he issue is whether fair notice requires the FTC to formally issue rules and regulations before it can file an unfairness claim in federal district court.") (emphasis omitted); JA21 ("[Wyndham's] arguments boil down to one proposition: the FTC cannot bring an enforcement action under

Section 5's unfairness prong without first formally publishing rules and regulations."); JA53 (framing issue as "[w]hether the [FTC] must formally promulgate regulations before bringing its unfairness claim under Section 5 of the [FTC] Act"). With all respect, that characterization of Wyndham's position is a straw man. Wyndham has never disputed the general principle that administrative agencies have discretion to regulate through either rulemaking or adjudication. *See*, *e.g.*, *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 290-95 (1974). Rather, Wyndham's point is only that, however an agency chooses to proceed, it must provide regulated entities with constitutionally requisite fair notice.

The district court held that the FTC had provided regulated entities with fair notice of the cybersecurity practices required by the statute for three basic reasons. *See* JA23-26. None has merit.

First, the court stated that "Section 5 codifies a three-part test that proscribes whether an act is 'unfair.'" JA23 (citing 15 U.S.C. § 45(n)); *see also* JA26 ("[A] statutorily-defined standard exists for asserting an unfairness claim."). As noted above, however, Section 5(n) does not set forth a test for "whether an act is 'unfair'"; rather, it

specifies that an act or practice is *not* "unfair" *unless* "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). But those limitations on the FTC's unfairness authority say nothing about data security, and thus in no way assist a business in determining whether its cybersecurity practices comply with the Act.

The district court insisted, however, that at common law, "liability is routinely found for unreasonable conduct *without* the need for particularized prohibitions." JA23 (emphasis in original). The short answer to that point is that liability under the FTC Act is not bounded by the common law. *See, e.g.*, *Sperry & Hutchinson*, 405 U.S. at 240-44; *FTC v. Motion Picture Adver. Serv. Co.*, 344 U.S. 392, 394 (1953); *R.F. Keppel*, 291 U.S. at 310-12. Because the common law does not limit the scope of the FTC Act, it follows that the common law cannot resolve the fair-notice issue here.

Second, the district court relied on "many public complaints" brought by the FTC challenging business cybersecurity practices, and "consent agreements" resolving such complaints. JA25. According to

the court, these complaints and consent agreements "'constitute a body of experience and informed judgment to which courts and litigants may properly resort for guidance.'" *Id.* (quoting *General Elec. Co. v. Gilbert*, 429 U.S. 125, 141-42 (1976) (emphasis omitted)).

But complaints and consent agreements are not adjudications on the merits, and "do[] not establish illegal conduct." *Intergraph Corp. v. Intel Corp.*, 253 F.3d 695, 698 (Fed. Cir. 2001). Because a complaint or a consent decree "is not a decision on the merits and therefore does not adjudicate the legality of any action by any party thereto," it does not and cannot provide fair notice of what the law either requires or proscribes. *Beatrice Foods Co. v. FTC*, 540 F.2d 303, 312 (7th Cir. 1976); *see also United States v. E.I. du Pont de Nemours & Co.*, 366 U.S. 316, 330 n.12 (1961) ("The circumstances surrounding ... negotiated [consent agreements] are so different that *they cannot be persuasively cited in a litigation context*.") (emphasis added). The decision to settle, rather than fight, an FTC complaint may reflect nothing more than a pragmatic business decision to avoid costly and protracted litigation.

And even if the Commission's prior cybersecurity complaints and consent agreements *could*, as a legal matter, provide fair notice (which

they cannot) the prior complaints and consent agreements at issue here contain only very general language that does not allow other regulated entities to ascertain what the law actually requires with respect to cybersecurity. Most of the complaints involve allegedly "deceptive" practices, and thus provide no guidance on what practices are allegedly "unfair." And most of the complaints fail to spell out what specific cybersecurity practices (or lack thereof) actually triggered the alleged violation; instead, they provide only a vague description of certain alleged problems that, "*taken together*," reflect a failure to provide "reasonable and appropriate" cybersecurity. *See*, *e.g.*, Compl. at 2, *In the Matter of EPN, Inc.*, FTC File No. 112 3143 (June 7, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/06/120607epncmpt.pdf; Compl. at 2, *In the Matter of Dave & Buster's, Inc.*, FTC File No. 082 3153 (Mar. 25, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100325davebusterscmpt.pdf; Compl. at 3, *In the Matter of Reed Elsevier, Inc. & Seisint, Inc.*, FTC File No. 052 3094 (Mar. 27, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080327complaint.pdf. And the consent agreements that do address unfairness do

so only in vague generalities. *See, e.g.*, Agreement Containing Consent Order at 2, *In the Matter of Dave and Buster's, Inc.*, FTC File No. 082 3153 (Mar. 25, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100325davebustersagree.pdf. (company agrees to implement "administrative, technical, and physical safeguards appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of the personal information collected from or about consumers").

Third, the court relied on the FTC's "business guidance brochure" regarding cybersecurity. JA25. But that brochure is a slim pamphlet that consists of such platitudes as: "LOCK IT. Protect the information that you keep." and "PLAN AHEAD. Create a plan to respond to security incidents." FTC, *Protecting Personal Information: A Guide for Business*, at 3 (Nov. 2011), *available at* http://www.business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf. The document contains little specific guidance on any particular cybersecurity practices, and nowhere states that its recommendations are required by law. Moreover, the pamphlet is rarely updated to reflect changes in the cybersecurity environment. For

instance, the most recent version of the document dates back nearly three years, to November 2011, and thus fails to reflect best practices gleaned from any of the recent high-profile data breaches that have plagued American businesses (not to mention the FTC itself) in recent years. *See*, *e.g.*, Hayley Tsukayama, *Neiman Marcus confirms data breach, offers few details*, Wash. Post, Jan. 11, 2014; *FTC sites hacked by Anonymous*, USA Today, Feb. 17, 2012. Given that this brochure does not even purport to establish what the law requires, it does not provide constitutionally adequate notice to regulated entities.

In effect, the district court read the constitutional fair-notice requirement out of the law with respect to the FTC Act. In particular, the court emphasized that "'the proscriptions in Section 5 are flexible, to be defined with particularity by the myriad of cases from the field of business.'" JA20 (quoting *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 385 (1965)); *see also* JA24 (same). To say that the FTC Act is not limited to particular practices, however, is not to say that the Act may be applied without regard for constitutional fair-notice principles. Rather, the Act may be applied to particular practices insofar as regulated entities were on notice that those practices were unlawful.

While a business may be charged with notice that it is unlawful, for instance, to advertise that a razor can shave sandpaper by showing a mock-up of plexiglass to which sand had been applied, *see Colgate-Palmolive*, 380 U.S. at 376, the same is not true of cybersecurity practices.

Contrary to the district court's assertion, Wyndham does not contend that "the FTC would have to cease bringing *all* unfairness actions without first proscribing particularized prohibitions—a result that is in direct contradiction with the flexibility necessarily inherent in Section 5 of the FTC Act." JA26 (emphasis in original). Wherever the precise line for constitutionally adequate notice may lie, this case is clearly on the wrong side of it. To say that Wyndham had constitutionally adequate notice that its cybersecurity practices were "unfair" in violation of the FTC Act is to write the constitutional fair-notice requirement out of the law.

III. The FTC Has Not Pleaded Sufficient Facts To State A Plausible Claim Of "Substantial" Injury To Consumers That Is Not "Avoidable" By Consumers.

Finally, above and beyond the substantial statutory and constitutional issues discussed above, the district court erred by

refusing to dismiss the FTC's complaint for failure to satisfy federal pleading standards. *See* JA26-34. Under those standards, a complaint "that offers 'labels and conclusions' or 'a formulaic recitation of the elements of a cause of action will not do.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 555). "Nor does a complaint suffice if it tenders 'naked assertion[s]' devoid of 'further factual enhancement.'" *Id.* (quoting *Twombly*, 550 U.S. at 557). Rather, "[t]o survive a motion to dismiss, a complaint must contain sufficient *factual* matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Id.* (emphasis added; quoting *Twombly*, 550 U.S. at 570); *see also id.* (complaint must "plead[] *factual* content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged") (emphasis added).

The complaint at issue here fails to plead any *facts* that would plausibly suggest a "substantial" injury to consumers that is not "avoidable" by consumers, as necessary to establish an "unfair" business practice. *See* 15 U.S.C. § 45(n). Indeed, the complaint fails to identify *any* consumer who suffered *any* financial injury as a result of the criminal cyberattacks on Wyndham. Rather, in a paragraph entitled

"**Total Impact of Breaches**," the complaint simply asserts, in conclusory terms, that the cyberattacks caused "substantial" consumer injury:

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

Am. Compl. ¶ 40, JA72-73.

As a threshold matter, the alleged exposure of a particular consumer's payment information, or a consumer's efforts to redress such exposure, do not give rise to a "substantial" injury—indeed, as this Court has held, such exposure and inconvenience do not even give rise to an injury sufficient to support Article III standing. *See*, *e.g.*, *Reilly v.*

Ceridian Corp., 664 F.3d 38, 42-46 (3d Cir. 2011); *see also Remijas v. Neiman Marcus Grp., LLC*, No. 14 C 1735, 2014 WL 4627893, at *3-4 (N.D. Ill. Sept. 16, 2014). Thus, the key allegations in Paragraph 40 are that the criminal cyberattack on Wyndham resulted in "fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss ... including, but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit." Am. Compl. ¶ 40, JA73. But the careful phrasing here is too clever by half.

The FTC does not, and cannot plausibly, allege that *consumers* suffered $10.6 million in "fraud loss." Federal law, after all, generally caps consumer liability for credit or debit card fraud at $50, *see* 15 U.S.C. §§ 1643(a)(1)(B), 1693g(a), and card brands go one step further by eliminating that liability altogether for both credit and debit cards.[7] Thus, as the FTC conceded at the hearing below, "[w]e are not saying $10.6 million in *unreimbursed* fraud charges." JA189 (emphasis added).

[7] *See* Visa, http://usa.visa.com/personal/security/zero-liability.jsp ("zero liability" for fraudulent charges); MasterCard, http://www.mastercard.us/zero-liability.html (same); American Express, https://www.americanexpress.com/us/content/fraud-protection-center/credit-card-fraud.html (same); Discover, http://www.discover.com/customer-service/fraud/protect-yourself.html (same).

To the extent that some consumers may have neglected to review their statements and paid the fraudulent charges without questioning them, that is the epitome of a "reasonably avoidable" injury that Section 5(n) excludes from the statute. 15 U.S.C. § 45(n). It is no accident, thus, that the complaint fails to allege any *facts*—as opposed to legal labels or conclusions—that would "allow[] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678.

The district court held otherwise by focusing on the reference in Paragraph 40 to "unreimbursed fraudulent charges." JA28. According to the court, "the FTC here alleges that at least some consumers suffered financial injury that included 'unreimbursed financial injury' and, drawing inferences in favor of the FTC, the alleged injury to consumers is substantial." *Id.* But that is not how federal pleading rules work. A court cannot just *speculate* that a plaintiff may be able to satisfy the relevant legal standard. Even if the complaint here adequately pleaded the existence of "unreimbursed fraudulent charges"—and, again, the complaint does not identify any—that would not satisfy the statute, as that would not explain why any such charges

were not "avoidable" by consumers (by simply asking their payment-card companies to reverse them), or how any such charges were "substantial." Indeed, to Wyndham's knowledge (and after extensive discovery), the FTC has been able to identify only a single consumer who was not fully reimbursed, and the amount of money at issue was $1.25 (one dollar and twenty-five cents). Because the complaint here pleads no facts that plausibly state a claim of "substantial" injury to consumers that is not "avoidable" by consumers, the district court should have dismissed the complaint on this ground too.

CONCLUSION

For the foregoing reasons, this Court should reverse the order denying Wyndham's motion to dismiss Count II of the FTC's amended complaint, and direct the district court to grant that motion.

October 6, 2014

Respectfully submitted,

/s/ *Eugene F. Assaf*

Eugene F. Assaf, P.C.
(DC Bar No. 449778)
Christopher Landau, P.C.
Susan M. Davies
K. Winn Allen
KIRKLAND & ELLIS LLP
655 Fifteenth St. N.W.
Washington, DC 20005
(202) 879-5000

Michael W. McConnell
STANFORD LAW SCHOOL
559 Nathan Abbott Way
Stanford, CA 94305
(650) 736-1326

Jennifer A. Hradil
Justin T. Quinn
GIBBONS P.C.
One Gateway Center
Newark, NJ 07102
(973) 596-4500

Douglas H. Meal
David T. Cohen
ROPES & GRAY LLP
800 Boylston Street
Boston, MA 02199
(617) 951-7000

Counsel for Appellant Wyndham Hotels & Resorts, LLC

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 9,684 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

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 Century Schoolbook.

October 6, 2014

/s/ *Eugene F. Assaf*
Eugene F. Assaf, P.C.
Counsel for Appellant

CERTIFICATE OF IDENTICAL COMPLIANCE OF BRIEFS

I, Eugene F. Assaf, P.C., hereby certify that the text of the electronically filed brief is identical to the text of the original copies that were dispatched on October 6, 2014, by Federal Express Overnight delivery to the Clerk of the Court of the United States Court of Appeals for the Third Circuit.

October 6, 2014

/s/ *Eugene F. Assaf*
Eugene F. Assaf, P.C.
Counsel for Appellant

CERTIFICATE OF BAR MEMBERSHIP

Pursuant to Local Appellate Rule 46.1(e), the undersigned hereby certifies that he is counsel of record and is a member of the bar of the United States Court of Appeals for the Third Circuit.

October 6, 2014

/s/ *Eugene F. Assaf*
Eugene F. Assaf, P.C.
Counsel for Appellant

CERTIFICATE OF PERFORMANCE OF VIRUS CHECK

I, Eugene F. Assaf, P.C., hereby certify that on October 6, 2014, I caused a virus check to be performed on the electronically filed copy of this brief using the following virus software: Microsoft Forefront Endpoint Protection, version 4.2.223.0. No virus was detected.

October 6, 2014

/s/ *Eugene F. Assaf*
Eugene F. Assaf, P.C.
Counsel for Appellant

CERTIFICATE OF SERVICE

I, Eugene F. Assaf, P.C., hereby certify that on October 6, 2014, I caused seven (7) copies of Appellant's Opening Brief to be dispatched by Federal Express Overnight delivery to the Clerk of the Court for the United States Court of Appeals for the Third Circuit, and filed an electronic copy of the brief via CM/ECF. I also caused a copy of this brief to be served electronically on the following counsel for Appellee:

Joel R. Marcus-Kurn, Esq. (*jmarcuskurn@ftc.gov*)
David C. Shonka, Esq. (*dshonka@ftc.gov*)
David L. Sieradzki, Esq. (*dsieradzki@ftc.gov*)
FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue, N.W.
Mail Stop H-584
Washington, DC 20580

October 6, 2014

/s/ *Eugene F. Assaf*
Eugene F. Assaf, P.C.
Counsel for Appellant