United States Court of Appeals

for the

Third Circuit

Case No. 14-3514

FEDERAL TRADE COMMISSION

– v–

WYNDHAM WORLDWIDE CORPORATION, a Delaware Corporation; WYNDHAM HOTEL GROUP, LLC, a Delaware limited liability company; WYNDHAM HOTELS AND RESORTS, LLC, a Delaware limited liability company; WYNDHAM HOTEL MANAGEMENT INCORPORATED, a Delaware Corporation

WYNDHAM HOTELS AND RESORTS, LLC,

Appellant

Appeal from an Order entered from the United States District Court for the District of New Jersey

AMICUS CURIAE BRIEF ON BEHALF OF APPELLANT WYNDHAM HOTELS AND RESORTS, LLC

JOHN F. COONEY
JEFFREY D. KNOWLES
MITCHELL Y. MIRVISS
LEONARD L. GORDON
RANDALL K. MILLER
VENABLE LLC
575 7th Street N.W.
Washington, DC 20004
(202) 344-4000

Counsel for Amicus Curiae Electronic Transactions Association

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Rules

Regulations

Miscellaneous

INTRODUCTION

Pursuant to Fed. R. App. P. 29 and 3d Cir. L.A.R. 29, the Electronic Transactions Association ("ETA") submits this brief *amicus curiae* in support of the position of Appellant Wyndham Hotels & Resorts, LLC ("Wyndham") that the district court erred, as a matter of law, in rejecting Wyndham's motion to dismiss Count II of the Amended Complaint, which alleged that Wyndham engaged in unfair business practices in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act").

The decision below turns business victims of cybercrime, including ETA's members, into perpetrators of an unfair trade practice under Section 5 of the FTC Act. In deeming cybercrime business victims to be the wrongdoers and not the victims, the decision tramples on a core limiting principle of the FTC Act requiring a "substantial injury" to consumers that consumers could not reasonably avoid to find a practice unfair. Congress took great pains to limit the Commission's authority under Section 5 to declare acts and practices as unfair, imposing strict requirements that only substantial consumer injuries could trigger FTC jurisdiction. The legislative history of this explicit decision by Congress makes clear that the Commission's attempt to expand its enforcement jurisdiction into cybersecurity here constitutes exactly the type of overreaching that Congress has criticized, and legislated against, for decades.

The decision below not only ignores this legislative context, but it makes short shrift of the three tests for an "unfair" act or practice under the FTC Act: a demonstration (1) that the act or practice causes, or will be likely to cause, substantial injury to consumers; (2) that the injury is not reasonably avoidable by consumers; and (3) that the injury is not outweighed by countervailing benefits to consumers or to competition. The FTC's action against Wyndham falls short on all three tests.

By operation of federal law, Wyndham consumers whose payment card data may have been exposed in a cybertheft did not, and could not, suffer substantial injury: they are by statute fully protected from fraud for all loss except for $50, and the major payment card networks, to further protect consumers, have agreed that they will not charge consumers for the minor loss not covered by federal law. Under this framework, consumers can protect against even that minor loss by simply reading their bills and reporting fraudulent transactions—making *any* losses quintessentially reasonably avoidable by consumers. Finally, given the negligible impact on consumers, the many burdensome consequences of vesting the Commission with expansive enforcement power far outweigh any interest in protecting consumers from the small losses that they actually suffer. The losses from cybertheft of consumer credit card data are borne by ETA's members and other businesses, not consumers, and the Commission should not be permitted to

expand its jurisdiction and impose significant burdens on businesses through its enforcement powers when consumers are not suffering the losses at issue.

STATEMENT OF IDENTITY, INTERESTS, AND AUTHORITY[1]

ETA is an international trade association representing more than 550 companies that offer electronic transaction processing products and services. The purpose of ETA is to influence, monitor, and help shape the payments industry by providing leadership through education, advocacy, and the exchange of information. ETA's membership spans the breadth of the payments industry, from independent sales organizations to financial institutions, from transaction processors to mobile payment technologies and equipment suppliers. Its members are dedicated to providing U.S. merchants and consumers the safest, most reliable, and most secure payments system to facilitate commerce and power our economy.

Recently, theft of electronic consumer payment card data by criminal hackers has highlighted the need to ensure the safety and security of consumer financial data. ETA has been an active participant in the ongoing legislative discussions about this serious problem, commenting on state laws and federal legislative efforts regarding data breaches and the protection of consumer

[1] Pursuant to Fed. R. App. P. 29(c)(5), ETA's counsel authored this brief. No counsel or party other than ETA, its members, or its counsel made a monetary contribution intended to fund the preparation or submission of this brief. ETA has no parent corporation, and no publicly held corporation owns 10% or more of ETA's stock.

information. Moreover, ETA and its members are intimately familiar with the statutory protections and requirements surrounding data security, especially as it relates to payment card information. Finally, ETA has a wealth of knowledge regarding self-regulatory standards and procedures that constitute the most effective method of preventing, mitigating, and recovering from cyberattacks and data breaches. ETA thus is well-positioned to provide this Court with important context on the relation between the theft of consumer payment card information and the protections available to consumers under federal law.

SUMMARY OF ARGUMENT

Cybertheft of consumer financial data constitutes a serious national problem that consumes significant resources and imposes tremendous costs on the economy. ETA's members and their merchant customers, not consumers, bear the financial burden when stolen payment information is used. Thus, ETA knows all too well the importance of this issue. But using Section 5 of the FTC Act against the companies that are themselves the direct victims of criminal cyberattacks is *not* the appropriate tool to deal with this policy problem.

While ETA takes no view on the appropriateness of the data security practices at issue in this case, ETA endorses Wyndham's cogent analysis of why the district court's analysis is legally wrong. First, as Wyndham explains at pages 18 to 35 of its Brief, Congress has not authorized the FTC to use Section 5 of the

FTC Act to police data security generally. Instead, Congress has authorized the agency to determine that a business practice is "unfair" only if it is likely to "cause substantial injury" to consumers. 15 U.S.C. § 45(n). As Wyndham correctly notes, the definition of "unfair" means that the practice must be "one 'marked by injustice, partiality or deception,' *i.e.*, one that is 'not equitable.'" Wyndham Br. 18 (quoting *Webster's Ninth New Collegiate Dictionary* (1988)). Wyndham's actions here did not seek to take advantage of consumers for its own benefit; rather, their interests were aligned in seeking to prevent disclosure of confidential information. Moreover, the injury (if any) that consumers suffered was not "caused" by Wyndham, but rather was caused by a criminal attack by foreign hackers, of which Wyndham was the direct victim. Under these circumstances, the FTC seeks to convert the unfairness power Congress actually enacted into some type of common law negligence theory on the ground that Wyndham failed to adopt some undefined safeguards for its data that the FTC believes are appropriate, given the nature and scope of its activities and the sensitivity of the information collected from consumers. *See Dave and Buster's, Inc.*, 149 F.T.C. 1449 (Mar. 25, 2010). Section 5(n), however, imposes strict limits on the FTC's unfairness authority and as a matter of law does not permit the agency to hold Wyndham liable under the theory alleged in the Complaint.

Second, as Wyndham explains at pages 35 to 45, even assuming the agency could proceed on such a theory, the FTC's failure to provide adequate notice of what constitutes reasonable data security violates basic notions of due process.

Third, as Wyndham explains at pages 45 to 50 and as explained further below, because of protections provided by federal statute and practices of the payment card networks, consumers whose payment information may be compromised in a cyberattack do not suffer substantial injury and, in any event, may reasonably avoid injury by the simple step of reviewing their payment card statements for charges they did not incur. Moreover, any possible slight consumer injury is outweighed by costs and burdens that would result by FTC intervention in the complex payments industry. As a result, the unfairness claims fail as a matter of law to satisfy the limits that Congress has placed on the FTC's use of its unfairness authority, and this Court should direct that Count II of the FTC's complaint be dismissed.

In this *amicus* brief, ETA sets forth the legislative and agency history documenting long-standing congressional concern with overreaching by the FTC, particularly with regard to the "substantial injury" requirement for proving unfairness under Section 5. Years ago, when Congress considered stripping the FTC of its unfairness authority, the FTC itself responded with a policy, the so-called Unfairness Policy Statement, which promised to limit FTC enforcement

activity to only acts or practices that caused substantial injuries to consumers. In this enforcement action, the FTC has abrogated that express commitment and instead is attempting to bring an enforcement action regarding an event that could have caused only *de minimis* injury to consumers. It thereby seeks to turn a business victim of the crime into a perpetrator of unfair trade practices merely because the victim failed to take steps adequate enough, in the FTC's hindsight vision, to prevent the crime from happening. This turns the "substantial injury" requirement and the FTC's Unfairness Policy Statement on their respective heads.

ETA's members and others in the card payment industry spend millions of dollars each year trying to prevent cyberattacks and bear the costs and responsibility for unauthorized charges. But the mere event of a cyberattack has no bearing on the FTC's authority in the absence of unavoidable and substantial *consumer* injury. The FTC should not be allowed to impose its policy prerogatives on broad sectors of the economy with unbounded discretion, especially in light of the FTC's hindsight-driven approach to data security.

This case demonstrates compellingly why the FTC has overstepped its statutory powers. The FTC Act, at 15 U.S.C. § 45(n), limits the FTC's authority to declare an act or practice unlawful to only those circumstances where the act or practice is unfair to consumers. For an act or practice to be "unfair," it must cause, or be likely to cause, substantial injury to consumers. In addition, such injury must

not be reasonably avoidable by consumers, and the injury must not be outweighed by countervailing benefits to consumers or to competition. The FTC action fails each of these tests.

First, both federal law and industry practice protect consumers whose payment card information is stolen through cybertheft, precisely to ensure that consumers do not suffer substantial injury. As Wyndham points out, the FTC has failed to show *any* substantial injury to *any* consumer in this case.

Second, even if *de minimis* harm were possible, consumers can reasonably avoid it by the simple step of reviewing their monthly statements and alerting their credit card companies of a fraudulent charge.

Third, because of industry practices any consumer harm is nonexistent or *de minimis,* that harm does not outweigh the burden that an FTC order would impose on Wyndham or any other victim of a cyberattack.

By ignoring the explicit statutory criteria that Congress adopted to limit the agency's authority under the unfairness prong of Section 5 and that the FTC accepted in its Unfairness Policy Statement, the district court essentially rewrote the statute and permitted the FTC to proceed on a theory that violates the literal provisions of the law. That decision should be reversed.

ARGUMENT

I. CONGRESS LIMITED THE FTC'S ABILITY TO INVOKE ITS UNFAIRNESS AUTHORITY TO SITUATIONS INVOLVING "SUBSTANTIAL INJURY" TO CONSUMERS THAT IS NOT REASONABLY AVOIDABLE.

Congress created the FTC's consumer protection unfairness authority with its insertion of the phrase "unfair acts or practices" into Section 5(a) of the FTC Act in the Wheeler-Lea Act of 1938, Pub. L. 447, 52 Stat. 111 (1938), *codified at* 15 U.S.C. § 45(a) (as amended). Previously, Section 5(a) had covered only unfair methods of competition.

In the late 1970s, the FTC began to use its unfairness authority aggressively to challenge a variety of practices against which it had not previously proceeded. *See* ABA Section of Antitrust Law, *Consumer Protection Law Developments* 58 (2009). These efforts culminated in the "kid vid" controversy, where the FTC sought to issue regulations regarding advertising to children. The controversy reached a level where the FTC was criticized as appointing itself the "nation's nanny," and Congress considered stripping the FTC of its unfairness authority. *Id.*

In response to these reactions to its unprecedented assertions of its authority, the FTC retreated from its efforts to promulgate regulations under its unfairness authority and issued, in the form of a letter to two senators, an Unfairness Policy Statement that it represented would guide its law enforcement efforts going forward. *See* Letter from the FTC to Sens. Wendell H. Ford & John C. Danforth

(Dec. 17, 1980), *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1070–76 (1984) (the "FTC Unfairness Policy"). In the Unfairness Policy Statement, the FTC made clear that two factors that it had previously considered in determining whether conduct was unfair were not independent bases for declaring conduct unfair—violations of public policy and unscrupulous or unethical business conduct. Rather, the FTC stated that a *substantial consumer injury* is necessary to make an act or practice unfair. The FTC then set forth what constitutes substantial consumer injury:

> The Commission is not concerned with trivial or merely speculative harms. In most cases, a substantial injury involves monetary harm. . . . Unwarranted health and safety risks may also support a finding of unfairness. Emotional impact and other more subjective types of harm, on the other hand, will not ordinarily make a practice unfair.

Id. at 1073.

In 1994, Congress ensured that the FTC would not backslide on its commitment to limit its unfairness authority to only those practices that caused substantial consumer injury. Thus, Congress added Section 5(n) to the FTC Act, which provides:

> The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be

> considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

15 U.S.C. § 45(n).

The limits that Congress placed on the FTC's use of its unfairness authority in 1994 require dismissal of the FTC's effort to use that authority in matters concerning data breaches involving consumer payment information for three reasons: first, there is no likelihood of substantial harm to consumers; second, any minimal harm that might occur is reasonably avoidable by the consumer; and third, any such minimal harm is outweighed by the costs sought to be imposed by the FTC on the companies that are already victims of the cyberattack.

Cyberattacks and cybersecurity are important national policy issues that affect ETA's members directly. ETA's members spend millions of dollars each year trying to prevent attacks. Its members and others in the card payment industry bear the costs and responsibility for unauthorized charges. Congress specifically directed, however, that policy concerns do not provide an adequate basis for finding a practice unfair in the absence of unavoidable and substantial *consumer* injury. To minimize or fail to rigorously apply the limits that Congress placed on the FTC's authority is to invite the FTC to impose its policy prerogatives on broad sectors of the economy with unbounded discretion. That problem is compounded

by the FTC's selective enforcement approach to data security. *See* Wyndham Br. 16.

II. THE FTC CANNOT SATISFY ITS BURDEN TO PLEAD SUBSTANTIAL CONSUMER INJURY.

Under Section 5(n) of the FTC Act, the Commission must first prove that consumers likely would be substantially injured by a company's data security practices; a speculative injury is insufficient. *See, e.g.*, *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011) (finding that speculative future harm does not meet Article III pleading standards in a data breach case). Thus, liability under the unfairness prong of Section 5 attaches only when the FTC can prove that the defendants' act is likely to cause substantial injury to consumers. *See FTC v. Neovi, Inc.*, 604 F.3d 1150, 1157 (9th Cir. 2010). Federal law and industry practice already protect consumers from being injured from the theft of payment card data, however, so no substantial consumer injury can arise from the type of data breach at issue in the present case.

Federal law ensures that consumers will not suffer substantial injury by placing a $50 limit on the amount for which a consumer can be liable for the unauthorized use of a payment card. *See* 15 U.S.C. § 1643(a)(1)(B). The express intent of Congress in enacting Section 1643(a)(1)(B) was to protect the consumer or cardholder against charges for unauthorized use of his or her credit card and to limit his or her liability for such unauthorized use. *See Martin v. Am. Express,*

Inc., 361 So. 2d 597, 600–01 (Ala. Civ. App. 1978). If a consumer challenges a transaction, the card issuer, not the consumer, faces the heavy burden of showing that the use of the card was authorized. *See* 15 U.S.C. § 1643(a)(1). Moreover, to further insulate consumers from injury, all of the major payment card networks have established a general policy of waiving liability even for that small amount.[2] Similarly, federal regulations issued by the Federal Reserve Board eliminate all consumer liability for unauthorized charges on debit cards, so long as the charges are reported within sixty days. *See* 12 C.F.R. § 205.6(b)(3). Taken together, these practices mean that the consumers whose information was illegally obtained by hackers in the Wyndham breaches are not responsible for even a cent of unauthorized charges.

---

[2] *See* American Express's Security Center, *Types of Fraud*, https://www.americanexpress.com/us/content/fraud-protection-center/credit-card-fraud.html (last visited Oct. 14, 2014) ("[R]emember, when you use your American Express® card, **you are not liable for fraudulent purchases**.") (emphasis added); Discover, *Understanding Fraud*, https://www.discover.com/ credit-cards/member-benefits/security-center/keep-secure/understand-fraud.html (last visited Oct. 14, 2014) ("remember that our $0 Fraud Liability Guarantee means **you are never responsible for unauthorized transactions** on your Discover card account") (emphasis added); Mastercard Worldwide, Zero Liability Protection, http://www.mastercard.us/zero-liability.html (last visited Oct. 14, 2014) ("Have peace of mind knowing that the bank that issued your MasterCard won't hold you responsible for 'unauthorized transactions.'"); Visa, *Zero Liability*, http://usa.visa.com/personal/security/zero-liability.jsp (last visited Oct. 14, 2014) ("Visa's Zero Liability policy is our guarantee that **you won't be held responsible for fraudulent charges** made with your card or account information") (emphasis added).

Therefore, under this current framework, the FTC cannot satisfy an essential element of an unfairness claim, to allege and prove substantial injury to consumers, regardless of whether the Commission defines it as substantial harm to a *few* consumers or broader, albeit smaller, harm to *many* consumers. *See* FTC Unfairness Policy Statement at 1073 n.12. Federal law precludes liability for over $50 for unauthorized charges, and all major credit card brands hold harmless all consumers, negating both notions of harm.

This lack of injury has been recognized in other cases. In *Reilly v. Ceridian Corp.*, this Court held that plaintiffs do not have standing in data breach cases "where no misuse is alleged" because "there has been no injury." 664 F.3d at 45. The Court, reasoning that the plaintiff's damages were speculative, rather than actual, dismissed the suit for failure to allege, let alone even prove, cognizable injury. *Id.* at 45. Indeed, this Court "has refused to confer standing when plaintiffs fail to allege an imminent injury-in-fact." *Id.* at 43. This principle can also be seen in *Remijas v. Neiman Marcus Grp., LLC*, No. 14 C 1735, 2014 U.S. Dist. LEXIS 129574 (N.D. Ill. Sept. 16, 2014), which ruled that allegations of "fraudulent charge[s]" resulting from stolen credit card information were insufficiently "concrete," as required for Article III standing. *Id.* at *11. As the plaintiffs did not allege that any of the fraudulent charges were unreimbursed, the court was "not persuaded that unauthorized credit charges for which none of the plaintiffs are

financially responsible qualify as 'concrete' injuries.'" *Id.* at *10. The court also noted that:

> Generally, when one sees a fraudulent charge on a credit card, one is reimbursed for the charge, and the threat of future charges is eliminated by the issuance of a new card . . . . If the complaint is to credibly claim standing on this score, it must allege something that goes beyond such *de minimis* injury.

Id. at *11–*12.

In the proceedings below, in tacit recognition of the protections against consumer harm established by federal law and the practices of the payment card networks, the FTC sought to establish substantial injury by relying on injuries "other than unreimbursed fraud," such as "frozen accounts" and "time and money resolving fraudulent charges." But courts in data-security cases have routinely rejected such attenuated and speculative injuries as not constituting actionable consumer harm—even in cases that do not apply the high "substantial injury" bar set by the FTC Act. *See Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 973 n.18 (D.C. Cir. 1985); *Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 8 (D.D.C. 2007). Here, given the FTC's burden of pleading facts showing substantial injury, the FTC's conclusory allegations of attenuated or speculative harm fail to state a claim, and Count II should have been dismissed for its failure to satisfy this essential element of the cause of action.

The district court distinguished *Reilly* by finding that Wyndham's actions "exposed consumers' personal information to unauthorized access[.]" (JA 72–73). This mere "exposure" to "unauthorized access" is not, by itself, sufficient to meet Section 5's requirement of *substantial* injury. At the very most, it is a wholly speculative—and highly unlikely—risk of a barely theoretically *possible* injury. No court nationwide has held that theft of one's credit card number, without more, constitutes an injury. Thus, the FTC cannot meet its "substantial injury" burden. *See Reilly*, 664 F.3d at 42 (finding no harm to consumers because plaintiffs' "credit card statements are exactly the same today as they would have been had Ceridian's database never been hacked"); *see also LaCourt v. Specific Media*, 8:10-cv-01256-GW-JCG, 2011 WL 1661532, at *4 (C.D. Cal. Apr. 28, 2011) ("it is categorically impossible for Plaintiffs to allege some property interest that was compromised by Defendant's [collection of personal information]"); *McLoughlin v. People's United Bank, Inc.*, No. 3:08-cv-00944 (VLB), 2009 WL 2843269, at *7 (D. Conn. Aug. 31, 2009) (agreeing that "the theft of personal data did not represent an ascertainable loss" sufficient to state a claim under state consumer protection law); *Willey v. J.P. Morgan Chase, N.A.*, No. 09 Civ. 1397 (CM), 2009 WL 1938987, at *4 (S.D.N.Y. July 7, 2009) (dismissing claim for FCRA violation where, "without providing a factual basis, [the plaintiff] appears to assert that a violation of the FCRA must have occurred simply because the data loss incident occurred"); *In re*

Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 131 n.128 (D. Me. 2009) ("[T]he cases that the parties cite are almost uniform in not allowing recovery where there is only a risk of injury and no actual misuse of the stolen electronic data."); *Shafran v. Harley-Davidson, Inc.*, No. 07 Civ. 01365 (GBD), 2008 WL 763177, at *3 (S.D.N.Y. Mar. 20, 2008) (granting motion to dismiss damages case resulting from data-security breach: "Courts have uniformly ruled that the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy. Plaintiff has not presented any case law or statute, from any jurisdiction, indicating otherwise. Plaintiff's alleged injuries are solely the result of a perceived and speculative risk of future injury that may never occur. Plaintiff has failed to show an actual resulting injury that might support a claim for damages.").

III. CONSUMERS COULD REASONABLY AVOID ANY INJURY FROM THE WYNDHAM DATA BREACH.

Under Section 5, the FTC also must show that consumers cannot reasonably avoid the injury in question. Therefore, to pursue its claims against Wyndham, or similar claims against other companies, the FTC must prove that consumers can neither avoid charges nor otherwise mitigate them. *Neovi*, 604 F.3d at 1158.

This limitation on the use of the unfairness authority reflects the congressional purpose underlying the unfairness doctrine—to protect consumers where the market fails and does not protect consumers. The FTC's Unfairness

Policy Statement and subsequent case law stand for the proposition that, as a threshold issue, the Commission may intervene through its unfairness authority only if consumers lack redress through the market. *See* FTC Unfairness Policy Statement at 1073–74. Put differently, the basis of "the reasonably avoidable inquiry is that free and informed consumer choice is the first and best regulator of the marketplace." *Porsche Cars N. Am., Inc. v. Diamond*, 140 So. 3d 1090, 1098–99 (Fla. Dist. Ct. App. 2014) (applying Florida's mini-FTC Act). The variety of protections available to consumers whose data may have been illegally accessed represents the quintessential "self-correcting" marketplace. *See Am. Fin. Servs. Ass'n*, 767 F.2d at 976. As discussed in *American Financial Services*, the Commission has statutory authority only when consumer injury is unavoidable because of some market failure. *See id.* (citing the FTC Unfairness Policy Statement). The court in *American Financial* found that consumer injury was not reasonably avoidable, based in part on the lack of competition among creditors whose services were at issue. *Id.* at 976–77. The exact opposite situation prevails in the payment card industry where the market has worked to the benefit of consumers and all of the major card issuers have agreed to hold consumers completely harmless for unauthorized charges.

"Reasonable avoidance" may be achieved through the consumer's prevention or mitigation of a harm. *See Orkin Exterm'g Co. v. FTC*, 849 F.2d

1354, 1365 (11th Cir. 1988) ("Consumers may act to avoid injury before it occurs if they have reason to anticipate the impending harm and the means to avoid it, or they may seek to mitigate the damage afterward if they are aware of potential avenues toward that end.") (citing the FTC Unfairness Policy).

In data breach cases, the available consumer protections under federal law and the absence of liability for fraudulent charges will forestall any possible substantial injury so long as consumers take the reasonable precautions of reading their payment card statements and notifying the payment card network of unauthorized charges. *Contra FTC v. Verity Int'l, Ltd.*, 335 F. Supp. 2d 479, 499 (S.D.N.Y. 2004) (finding that FTC had shown that injury could not be reasonably avoided where consumers were required "first to suffer an injury and then to find and implement a solution to avoid being injured again"). Rather, federal law and the payment card networks, in response to competitive pressures, have removed the possibility of substantial harm to consumers as a result of fraudulent payment card charges, thus eliminating the need for cumbersome and expensive regulatory intervention.

To avoid an unauthorized charge resulting from the theft of payment card data in a cyberattack, a consumer simply must notify the company that issued the card that a charge was not authorized. Such a simple step is the quintessence of a

consumer reasonably avoiding an injury. To find otherwise is to read out of the statute this restriction that Congress placed on the FTC's authority.

IV. ANY ACTUAL INJURY TO CONSUMERS IS OUTWEIGHED BY THE BURDENS THAT FTC ENFORCEMENT PLACES ON WYNDHAM AND THE ECONOMY GENERALLY.

The FTC also must prove that any consumer injury, in addition to being substantial, outweighs any countervailing benefits to consumers or competition. *See FTC v. J.K. Publ'ns, Inc.*, 99 F. Supp. 2d 1176, 1201 (C.D. Cal. 2000). That inquiry also includes the costs of the remedy to the defendant and to the economy in general. *See Int'l Harvester Co.,* 104 F.T.C. 949, 1070 (1984) (stating that the FTC must broadly account for "the various costs that a remedy would entail," including "the costs to the parties directly before the agency") (quoting Unfairness Policy Statement).

In the unique environment of payment card liability law, which holds consumers harmless from unauthorized charges, the burden of any FTC injunctive relief would significantly outweigh the nonexistent, noncognizable harm purportedly suffered by consumers. While consumer loss is nonexistent or minimal, the burdens of an FTC remedy are real and substantial. To comply with typical FTC injunctive relief, an FTC data security defendant must, typically for twenty years, pay internal and independent personnel to monitor its compliance with an injunction or a consent decree, record that compliance, undertake and pay for professional audits to test that

compliance, and report proof of that compliance. *See, e.g.*, *Dave & Buster's, Inc.*, 149 F.T.C. 1453 (June 8, 2010) (Decision and Order); *TJX Companies, Inc.*, Dkt. No. C-4227, Decision and Order (F.T.C. Aug. 1, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxdo.pdf. The direct and indirect costs of such a program more than tip the scales in Wyndham's favor.

The burden of an FTC remedy is further heightened because of the complex requirements that already exist regarding payment card data. The card payment industry maintains a strict standard through the Payment Card Industry Data Security Standards ("PCI DSS"), subject to verified compliance audits on an annual basis.[3] Burdening companies with another potentially conflicting layer of compliance obligations and possible penalties is unnecessary, given the absence of consumer harm, and does little good, even siphoning resources that would otherwise be spent on making systems and processes more secure.

[3] *See* PCI Standards Security Council, Payment Card Industry Security Standards Overview (2008), https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf.

CONCLUSION

Cyberattacks and data security remain a serious problem. The FTC's effort to use its unfairness authority in this arena does not solve or mitigate the problem, and the allegations in Count II do not state a claim because they violate limits that Congress has placed on the agency's unfairness authority. For the foregoing reasons, 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.

October 14, 2014

Respectfully Submitted,

/s/ John F. Cooney

John F. Cooney (Counsel of Record)
Jeffrey D. Knowles
Mitchell Y. Mirviss
Leonard L. Gordon
Randall K. Miller
VENABLE LLC
575 7th Street N.W.
Washington, DC 20004

Counsel for Amicus Curiae
Electronic Transactions Association

CERTIFICATE OF BAR MEMBERSHIP

I certify, pursuant to 3d Cir. L.A.R. 28.3(d), that I am a member of the Bar of this Court.

/s/ John F. Cooney
John F. Cooney

Counsel for Amicus Curiae
Electronic Transactions Association

CERTIFICATE OF COMPLIANCE WITH FEDERAL RULE OF APPELLATE PROCEDURE 32(a) AND LOCAL RULE 31.1

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify the following:

This brief complies with the type-volume limitation of Rule 32(a)(7)(B) of the Federal Rules of Appellate Procedure because this brief contains 4,994 words, excluding the parts of the brief exempted by Rule 32(a)(7)(B)(iii) of the Federal Rules of Appellate Procedure.

This brief complies with the typeface requirements of Rule 32(a)(5) of the Federal Rules of Appellate Procedure and the type style requirements of Rule 32(a)(6) of the Federal Rules of Appellate Procedure because this brief has been prepared in a proportionally spaced typeface using the 2008 version of Microsoft Word in 14 point Times New Roman font.

This brief complies with the electronic filing requirements of Local Rule 31.1(c) because the text of this electronic brief is identical to the text of the paper copies, and the Vipre Virus Protection, version 3.1 has been run on the file containing the electronic version of this brief and no viruses have been detected.

Dated: October 14, 2014

/s/ John F. Cooney
John F. Cooney

AFFIDAVIT OF SERVICE

DOCKET NO. 14-3514
----------X
Federal Trade Commission

vs.

Wyndham Worldwide Corp.
----------X

I, Elissa Matias, swear under the pain and penalty of perjury, that according to law and being over the age of 18, upon my oath depose and say that:

On October 14, 2014

I served the within Amicus Curiae Brief on behalf of Appellant Wyndham Hotels and Resorts, LLC in the above captioned matter upon:

See Attached Service List

via **electronic filing and electronic service**.

Unless otherwise noted, copies have been sent to the court on the same date as above for filing via Express Mail.

Sworn to before me on October 14, 2014

/s/ Robyn Cocho
Robyn Cocho
Notary Public State of New Jersey
No. 2193491
Commission Expires January 8, 2017

/s/ Elissa Matias
Elissa Matias

Job # 256043

SERVICE LIST

Joel R. Marcus, Esq.
Email: jmarcuskurn@ftc.gov
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554
(202) 418-1745

David C. Shonka, Sr.
Email: dshonka@ftc.gov
David L. Sieradzki, Esq.
Email: dsieradzki@ftc.gov
Federal Trade Commission
H-584
600 Pennsylvania Avenue, N.W.
Washington, DC 20580
(202) 326-2436

Kenneth W. Allen, Esq.
Email: winn.allen@kirkland.com
Eugene F. Assaf, Esq.
Email: eugene.assaf@kirkland.com
Christopher Landau, Esq.
Email: christopher.landau@kirkland.com
Susan M. Davies, Esq.
Email: susan.davies@kirkland.com
Kirkland & Ellis
655 15th Street, N.W.
Suite 1200
Washington, DC 20005
(202) 879-5200

David T. Cohen, Esq.
Email: david.cohen@ropesgray.com
Ropes & Gray
1211 Avenue of the Americas
New York, NY 10036
(212) 841-8880

Jennifer A. Hradil, Esq.
Email: jhradil@gibbonslaw.com
Justin T. Quinn, Esq.
Email: jquinn@gibbonslaw.com
Gibbons
One Gateway Center
Newark, NJ 07102
(973) 596-4495

Michael W. McConnell, Esq.
Email: michael.mcconnell@kirkland.com
STANFORD LAW SCHOOL
559 Nathan Abbott Way
Stanford, CA 94305
(650) 736-1326

Douglas H. Meal, Esq.
Email: douglas.meal@ropesgray.com
Ropes & Gray
800 Boylston Street
Prudential Tower
Boston, MA 02199
(617) 951-7517