UNITED STATES COURT OF APPEALS FOR THE THIRD CIRCUIT

Case No. 14-3514

FEDERAL TRADE COMMISSION,

Plaintiff - Appellee,

v.

WYNDHAM WORLDWIDE CORP.; WYNDHAM HOTEL GROUP, LLC; WYNDHAM HOTELS & RESORTS, LLC; AND WYNDHAM HOTEL MANAGEMENT, INC.,

Defendants - Appellants.

On appeal from the United States District Court
for the District of New Jersey
(Hon. Esther Salas, United States District Judge)

BRIEF OF AMICI CURIAE PUBLIC CITIZEN, INC., CENTER FOR DIGITAL DEMOCRACY, AND CONSUMER ACTION IN SUPPORT OF PLAINTIFF-APPELLEE FEDERAL TRADE COMMISSION URGING AFFIRMANCE

Jehan A. Patterson
Scott Michelman
PUBLIC CITIZEN LITIGATION GROUP
1600 20th Street NW
Washington, DC 20009
(202) 588-1000

Attorneys for Amici Curiae Public Citizen, Inc., et al.,

November 12, 2014

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1 & 29(c)(1), amici curiae Public Citizen, Inc., Center for Digital Democracy, and Consumer Action state that they have no parent corporation and that there are no publicly held corporations that own 10% or more of amici.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

ADMINISTRATIVE MATERIALS

MISCELLANEOUS

INTEREST OF AMICI CURIAE

Public Citizen, Inc., a non-profit advocacy organization with more than 300,000 members and supporters nationwide, appears before Congress, federal agencies, and the courts to advocate for openness in government, access to courts, consumer protections, and health and safety regulations. Since its founding more than forty years ago, Public Citizen has appeared frequently as a party or amicus curiae in cases around the country to advocate for increased consumer protections and stronger regulatory authority across a variety of industries, including in cases involving the Federal Trade Commission (FTC), *e.g.*, *North Carolina Board of Dental Examiners v. FTC*, No. 13-534 (S. Ct.) (counsel for amicus curiae supporting FTC action alleging that dental licensing board engaged in anti-competitive conduct and was not entitled to state action immunity); *FTC v. Actavis, Inc.*, 133 S. Ct. 2223 (2013) (counsel for amicus curiae supporting FTC antitrust action concerning anti-competitive deals between brand-name and generic drug manufacturers); and cases involving protection of data and individual privacy, e.g., *Lane v. Facebook, Inc.*, 696 F.3d 811 (9th Cir. 2012) (counsel for objectors to class-action settlement concerning Facebook privacy settings); *In re TD Ameritrade Accountholder Litigation*, 266 F.R.D. 418 (N.D. Cal. 2009) (counsel for class member in case arising out of data breach that exposed consumer information). Public Citizen also submitted an amici curiae brief in the district

court proceedings in this case. The theft of consumers' personal information from a company's computer network significantly increases the risk that those consumers will become victims of identity fraud and suffer substantial injuries. Public Citizen believes that FTC enforcement actions against companies that fail reasonably to protect the security of their computer systems, thus rendering their systems vulnerable to breaches in which consumer data can be stolen, are critical as corporate data breaches continue to increase.

The Center for Digital Democracy (CDD) is recognized as a leading national consumer protection and privacy organization. CDD's public education programs are focused on informing consumers, policymakers, and the press about contemporary digital marketing and data collection issues, including their impact on public health, children, and youth, and financial services. CDD's focus on digital consumer protection in the modern day leads to its direct interest in this case. The FTC's oversight of online privacy and data protection are linked issues that must be upheld for the protection of American consumers who increasingly use technology to navigate their lives. In light of the increasing number of data breaches and companies holding large portfolios of consumer information that can be lost in such mishaps, now more than ever the FTC must be allowed to do its job and stop companies from giving up Americans' sensitive information. CDD sees

this as a central point to the future of the online marketplace and people's ability to protect themselves from cybercrime and privacy invasions.

Consumer Action is a 501(c)(3) non-profit organization that has championed the rights of underrepresented consumers nationwide since 1971. Throughout its history, the organization has dedicated its resources to promoting financial empowerment, consumer literacy, and basic fairness in consumer dealings with business. Consumer Action is deeply committed to ensuring that the interests of underrepresented consumers are protected by consumer protection laws and agencies, such as the FTC, and it has a longstanding interest in protecting the consumer protection authority of these agencies to enforce unfair acts and practices. In addition, Consumer Action has, since 2001, strived to educate consumers about privacy rights and fraud prevention, and to ensure that they are not victimized by acts or practices in the marketplace.

All parties have consented to the filing of this brief. No counsel for any party authored this brief in whole or part. Apart from amici curiae Public Citizen, et al., no person, including parties or parties' counsel, contributed money intended to fund the preparation and submission of this brief.

SUMMARY OF ARGUMENT

When consumers transact business online, they entrust sensitive information—financial, medical, and other personal data, such as birthdates and

even Social Security numbers—to the companies with which they do business. Recognizing the value of such consumer information, criminals seek to exploit vulnerabilities in companies' computer systems.

Sensitive consumer data such as credit or debit card numbers, bank account information, and Social Security numbers command large sums on the black market, as criminals can use this information to drain funds from bank accounts, make fraudulent purchases, apply for credit, and wrongfully obtain tax refunds or other government benefits. When such information is stolen, consumers expend money and time to, for example, dispute fraudulent transactions, notify their creditors of the identity fraud, and repair their credit. In some instances, consumers may be denied employment because of a damaged credit report, be unable to obtain low-cost credit, or be denied access to credit entirely, events that impair their chances of attaining or building their wealth through conventional means such as purchasing a home or financing an education. For these reasons, the Wyndham Appellants' argument that the FTC did not plausibly plead a substantial injury to consumers has no merit.

Although the injuries resulting from a data breach can be significant, private tort suits alleging such injuries are difficult to bring, and federal courts to date have not recognized a private remedy for consumers against companies where the companies' failure to adequately ensure against network breaches enables theft of

consumers' data but that data has not yet been misused, to the consumers' knowledge. Thus, FTC enforcement actions pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45, against companies that fail reasonably to protect their consumers' information from misappropriation are currently the only effective means of redressing the unfair corporate practices that lead to corporate data breaches that cause substantial injuries to consumers.

Here, the Wyndham Appellants had fair notice that their failure to maintain adequate data security practices could render them liable for unfair business practices under the FTC Act. For more than a decade, the FTC has publicly pursued enforcement actions pursuant to its statutory authority to enjoin unfair practices or acts against companies with similarly lax data security protocols.

ARGUMENT

I. Consumers Suffer Substantial Harm From Theft Of Their Financial And Personal Data.

A. Sensitive Consumer Information Is at Risk of Theft from Corporate Data Breaches.

Recent years have seen a number of high-profile corporate data breaches involving millions of compromised consumer records. *See* Jordan Robertson, *Customers Stay Despite High-Profile Data Breaches*, USA Today, May 2, 2011; *see also* Privacy Rights Clearinghouse, *Data Breaches: A Year in Review*, Dec. 16,

2011.[1] Among the most prominent are the breaches leading to theft of the personal information of tens of millions of cardholders and other customers from the computer systems of Target, Maggie McGrath, *Target Data Breach Spilled Info On As Many As 70 Million Customers*, Forbes, Jan. 10, 2014, Home Depot, Maggie McGrath, *Home Depot Confirms Data Breach, Investigating Transactions from April Onward*, Forbes, Sept. 8, 2014, and JPMorgan Chase. Emily Glazer and Danny Yadron, *J.P. Morgan Says About 76 Million Households Affected by Cyber Breach*, The Wall Street Journal, Oct. 2, 2014.[2] An annual study by Verizon, in tandem with national and international law enforcement agencies, data security researchers, and forensic auditors, confirmed 1,367 data breaches in 2013, Verizon, *2014 Data Breach Investigations Report* 2,[3] an increase of 120 percent over the previous year. Verizon, *2013 Data Breach Investigations Report* 11.[4]

---

[1] *Available at* http://usatoday30.usatoday.com/tech/news/2011-05-02-online-privacy_n.htm, and https://www.privacyrights.org/data-breach-year-review-2011.

[2] *Available at* http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/ (approximately 70 million Target customers' information was compromised), and http://www.forbes.com/sites/maggiemcgrath/2014/09/08/home-depot-confirms-data-breach-investigating-transactions-from-april-onward/; http://online.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372 (customers' names, email addresses, phone numbers, and addresses were stolen, affecting approximately 76 million American households).

[3] The full report is available at http://www.verizonenterprise.com/DBIR/2014/.

[4] The full report is available at http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

Hackers who breach corporate computer networks or websites to steal consumer data do not necessarily exploit the information themselves by making fraudulent purchases or applying for credit. Instead, consumer information is bought and sold in bulk, as "[t]he most successful identity thieves have learned that it's more lucrative to hack into businesses, where they can steal card numbers by the thousands or even millions," with each credit card number fetching a sale price of anywhere from ten to several hundred dollars. J. Craig Anderson, *Identity Theft Growing, Costly to Victims*, USA Today, Apr. 14, 2013.[5] Because the "crime profits [from data theft] can be staggering," Greg Farrell & Michael A. Riley, *Hackers Take $1 Billion a Year As Banks Blame Their Clients*, Bloomberg, Aug. 4, 2011,[6] attacks on corporate computer networks show no signs of abating.

B. The Fraudulent Use of Consumer Information Causes Significant Harm to Consumers.

The consequences of misappropriated consumer information are wide-ranging and extend far beyond the inconvenience of a cancelled credit card. One in three consumers who were notified by a company that their data was stolen became a victim of identity fraud in 2013. Blake Ellis, *Identity fraud hits new victim every*

[5] *Available at* http://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179.

[6] *Available at* http://www.bloomberg.com/news/2011-08-04/hackers-take-1-billion-a-year-from-company-accounts-banks-won-t-indemnify.html.

two seconds, CNN Money, Feb. 6, 2014.[7] Indeed, identity fraud has been the top consumer complaint to the FTC for 14 consecutive years. FTC, *Identity theft tops list of consumer complaints for 14th consecutive year*, Feb. 27, 2014.[8]

Consumers experience direct economic and opportunity costs in attempting to avoid identity theft. Proactive consumers who wish to prevent fraudulent use of their information upon learning of a data breach may place a freeze on their credit reports—for a price—to prevent prospective creditors from accessing their reports or credit scores without permission. With a freeze in place, however, they are themselves unable to obtain immediate credit, such as store credit cards, or a mortgage refinance. Michelle Singletary, *Protect your credit by freezing it*, The Washington Post, Jan. 21, 2014.[9] Further, consumers whose information has been stolen understandably find it necessary to purchase credit card insurance or credit repair services. *See* Jason Fitterer, *Putting a Lid on Online Dumpster-Diving: Why the Fair and Accurate Credit Transactions Act Should Be Amended to Include E-Mail Receipts*, 9 Nw. J. Tech. & Intellectual Prop. 591, 9 (2011) (estimating that

[7] *Available at* http://money.cnn.com/2014/02/06/pf/identity-fraud/ (citing Javelin Strategy & Research, *2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends*, https://www.javelinstrategy.com/ brochure/314).

[8] *Available at* http://www.consumer.ftc.gov/blog/identity-theft-tops-list-consumer-complaints-14th-consecutive-year.

[9] *Available at* http://www.washingtonpost.com/business/protect-your-credit-by-freezing-it/2014/01/21/cdf7b5d2-82d1-11e3-9dd4-e7278db80d86_story.html (estimating fees to place or lift a freeze to range from $2 to $10).

consumers spend approximately $7.5 billion annually on these products and services). And for those consumers whose credit or debit card information is used in fraudulent transactions, the "loss of time in dealing with problems associated with [the misuse] such as bounced checks, loan denials, credit card application rejections, debt collection harassment, insurance rejections, and the shut-down of utilities" is significant. S. Jacob Carroll, *FAA v. Cooper: Bombarding the Privacy Act with the "Canon of Sovereign Immunity,"* 64 Mercer L. Rev. 785, 804 (2013) (internal quotation marks and citation omitted).

Even data breaches where only names and email addresses are stolen can be harmful, as the information may be used to probe for more data on those consumers, thus increasing the likelihood that the consumers will be targeted for a phishing scheme that may lead to identity fraud. *See Patco Constr. Co., Inc. v. People's United Bank,* 684 F.3d 197, 204 n.5 (1st Cir. 2012) (in phishing scheme, "perpetrator will provide an e-mail or link that directs the victim to enter or update personal information at a phony website that mimics an established, legitimate website which the victim either has used before or perceives to be a safe place to enter information").

Most significantly, because "very little [personal] information is required to obtain credit, an identity thief can open numerous fraudulent accounts with information as basic as a social security number matched with an approximate

name and birth date." Eric T. Glynn, *The Credit Industry and Identity Theft: How to End an Enabling Relationship*, 61 Buffalo L. Rev. 215, 223 (2013). In such instances, victims "can spend years trying to resolve bad debt run up by thieves in their names." Anderson, *supra* n.5. In 2012 alone, identity fraud victims spent an average of 20 hours and approximately $776 to resolve such fraud. Herb Weisbaum, *Data Breaches Cost Consumers Billions of Dollars*, Today Money, June 5, 2013.[10] The costs of resolving identity fraud affect lower-income people disproportionately, with consumers earning less than $15,000 annually spending twice the amount of time and money addressing credit issues as consumers earning more than $150,000 per year. Consumers Union, *Fact Sheet About ID Theft*.[11]

On top of the expenditure of time and financial resources necessary to resolve a fraud dispute, the fall-out from a damaged credit report can be devastating. Victims of identity fraud may be denied loans for housing or education or lose employment opportunities, *see* Glynn, 61 Buffalo L. Rev. at 225, or be unable to rent an apartment, pay higher car insurance premiums or access sources of credit only at higher interest rates. *See* Experian, *Identity Theft Impact*

---

[10] *Available at* http://www.today.com/money/data-breaches-cost-consumers-billions-dollars-6C10209538 (citing Javelin Strategy & Research, *2013 Data Breach Fraud Impact Report: Mitigating a Rapidly Emerging Driver of Fraud* (June 2013)).

[11] *Available at* http://www.defendyourdollars.org/pdf/defendyourdollars.org-fact_sheet_about_id_theft.pdf.

on Credit Score.[12] The ramifications are not solely pecuniary, as the emotional distress caused by a damaged credit history can be severe. *See, e.g.*, *Cortez v. Trans Union, LLC*, 617 F.3d 688, 719 (3d Cir. 2010) (affirming award of compensatory damages for emotional distress caused by credit report alert erroneously identifying plaintiff as appearing on government list of known or suspected terrorists); *Dennis v. BEH-1, LLC*, 520 F.3d 1066, 1069 (9th Cir. 2008) (recognizing emotional distress caused by erroneous credit report to be "actual damages); *see also* Fitterer, 9 Nw. J. of Tech. and Intellectual Prop. at 10. Even worse, because there may be a considerable delay between the occurrence of a corporate data breach and the point at which that data is misused to the detriment of the consumer, and between the first date of misuse and the date of discovery, *see* FTC, *2006 Identity Theft Survey Report* 23 (2007) (indicating that one-quarter of victims of existing credit card fraud in one survey did not discover misuse for more than one month after the date of the first misuse and that three percent did not discover the misuse for six months or more),[13] injury following a data breach is very difficult if not impossible for a consumer to prevent.

---

[12] *Available at* http://www.protectmyid.com/identity-theft-protection-resources/identity-basics/credit-score-impact.aspx.

[13] *Available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-2006-identity-theft-survey-report-prepared-commission-synovate/synovatereport.pdf.

In their brief, the Wyndham Appellants downplay the harm to consumers flowing from the three breaches of Wyndham's computer networks by focusing solely on whether the consumers have incurred fraudulent charges on their credit or debit cards. *See* Appellants' Br. 48 & n.7 (noting that federal law and card issuer policies limit a consumer's liability for unauthorized charges (citing 15 U.S.C. § 1643(a)(1)(B))). But the Wyndham Appellants fail entirely to address the FTC's allegations that consumers suffered "increased costs, … lost access to funds or credit … [and] also expended time and money resolving fraudulent charges and mitigating subsequent harm." *Id*. at 47 (citing JA72-73 at ¶ 40). As explained above, these costs are not insubstantial. To avoid fraudulent charges, a consumer could place a freeze on her credit, but that would deprive her of access to immediate credit. If instead she wished to avoid losing access to credit, she could opt against placing a freeze on her credit, but then would face the risk that her sensitive personal or financial information could be used to incur fraudulent charges or open fraudulent accounts for credit. She thus would incur harm in the form of time and expenses spent disputing fraudulent charges or repairing a credit report. And in some cases, the consumer would have to pay to clear her credit reports. Chris Jay Hoofnagle, *Internalizing Identity Theft*, 13 UCLA J.L. & Tech. 2, at *23 (2009). In addition, consumers suffer damage to credit history caused by

the fraudulent activity (and the corresponding harms flowing from that damage) and emotional distress.[14]

The Wyndham Appellants' reliance on *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), to argue that no substantial consumer injury occurred in this case misses the mark. There, this Court held that consumers suing a company because their "information *may* have been accessed" in a data breach lacked standing to sue for "an increased risk of identity theft resulting from a security breach" because the risk was "too speculative." *Id.* at 43. Unlike this case, it was "not known whether the hacker read, copied, or understood the data," only "that a firewall was penetrated." *Id.* at 40, 44. Here, in contrast, consumer data was exported to a domain registered in Russia, JA 70 at ¶ 32, and misused to incur fraudulent charges, JA 71-72 at ¶¶ 34, 39. *Reilly* does not suggest that, in these circumstances, consumer injury has not occurred.

The Wyndham Appellants make much of the fact that they, too, were victims when hackers broke into their computer systems to steal customers' data.

[14] Injury from identity fraud is not borne solely by individual consumers. The Treasury Inspector General for Tax Administration estimates that the Internal Revenue Service will pay "as much as $21 billion in fraudulent tax refunds over the next five years as a direct result of" identity fraud. *Identity Theft and Tax Fraud: Growing Problems for the Internal Revenue Service, Part 4*: *Hearing Before the Subcomm. on Government Organization, Efficiency and Financial Management of the H. Comm. on Oversight and Government Reform*, 112th Cong. 2 (2012) (statement of Rep. Platts, Chairman, House Subcomm. on Government Organization, Efficiency and Financial Management).

But that point is irrelevant to whether the FTC may enforce its statutory mandate to police unfair corporate practices that are likely to cause substantial injuries to consumers. Moreover, the breaches of the Wyndham Appellants' system were perpetrated, not to injure them, but as a means of stealing valuable consumer information. For this reason, Wyndham cannot reasonably analogize FTC enforcement in the data security arena to regulation of the physical security of businesses. Appellants Br. 22-23. In the case of burglary or robbery of a business, thieves target the business's own property for damage or theft. But as the recent spate of corporate data breaches has demonstrated, with regard to data security, thieves do not seek business information, but consumer information. And although businesses lose "an estimated $150 to $250 for each card number stolen … in the form of legal settlements, fees for consultants hired to remove malware, and personnel hours spent notifying customers," those costs are not the purpose for the theft, and, moreover, "are passed on to consumers in the form of higher retail prices and credit-card fees." Anderson, *supra* n.5.

Because the theft of consumer data obtained in a data breach is likely to, and often does, cause substantial harm to consumers, this Court should affirm the decision below.

II. FTC Enforcement Actions Currently Provide The Most Effective Mechanism To Redress Unfair Data Security Practices That Result In Breaches Of Business Computer Networks.

FTC enforcement proceedings pursuant to 15 U.S.C. § 45 both deter and redress inadequate corporate data security practices. Notwithstanding that a data breach of a corporate computer system can and does result in substantial injuries to consumers, several federal courts, including the Third Circuit, have held that consumers whose information has been stolen but not (yet) misused either lack standing to bring claims against companies that failed adequately to protect their information or fail to state a claim. *See, e.g.*, *Reilly*, 664 F.3d at 45 (holding that, without alleging misuse of information, plaintiffs lacked standing because their "credit card statements are exactly the same today as they would have been had [the corporate] database never been hacked"); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 637 (7th Cir. 2007) (dismissing case because pleading damages for credit monitoring services insufficient to state breach of contract and negligence claims against bank that failed to secure consumer data where consumers had not suffered financial loss to their accounts or been victims of identity theft); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 656 (S.D. Ohio 2014) (holding that increased risk that plaintiffs would become victims of identity fraud as a result of defendant's data breach was not injury-in-fact for standing purposes); *Hammond v. The Bank of N.Y. Mellon Corp.*, No. 08-cv-6060, 2010 WL 2643307, at *2, *7

(S.D.N.Y. June 25, 2010) (dismissing common-law and statutory consumer protection claims for lack of standing where only injury alleged was increased risk of identity theft); *Allison v. Aetna, Inc.*, No. 09-cv-2560, 2010 WL 3719243, at *4 n.3 (E.D. Pa. Mar. 9, 2010) (collecting cases holding plaintiffs lacked standing); *Hinton v. Heartland Payment Sys., Inc.*, No. 09-cv-594, 2009 WL 704139, at *1 (D.N.J. Mar. 16, 2009) (finding that plaintiff failed to plead an actual injury because data had not been misused).

Perhaps because of the absence of a private enforcement mechanism, "[m]ost merchants are content to clean up the damage from an attack, rather than pay for better preventive measures." Anderson, *supra* n.5. Administrative enforcement by the FTC is therefore necessary to protect consumers, as it prompts companies to take adequate measures to secure their computer systems and to safeguard consumer information. It also serves as a critical remedial backstop while private challenges to consumer data breaches mature and while injuries underlying private claims develop.

Appellants concede that the FTC has the authority to regulate by adjudication, rather than formal rulemaking. *See* Appellants' Br. 39. And as compared to rulemaking, adjudication is better able to be responsive to data breaches and effective in policing corporate data security protocols and minimizing the damage to consumers from data breaches. The cybersecurity landscape is

evolving, as Appellants recognize, *see* Appellants' Br. 43, and data security standards promulgated through rulemaking may become outdated too quickly to be effective.

Nonetheless, the Wyndham Appellants' claim that they are alleged to have violated "an unknown (and unknowable) standard," Appellants' Br. 36, has no merit. As the cases they cite make clear, a regulated party may be deemed to have fair notice of an agency's statutory or regulatory interpretation where an agency's public statements or pre-enforcement efforts would allow it "to identify, with 'ascertainable certainty,' the standards with which the agency expects parties to conform …." *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1329 (D.C. Cir. 1995) (citation omitted); *cf. FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2318 (2012) (finding that regulatory history made clear that agency's indecency policy at time television broadcasts aired would not have applied to conduct at issue); *PMD Produce Brokerage Corp. v. U.S. Dep't of Agriculture*, 234 F.3d 48, 53 (D.C. Cir. 2000) (finding no public statements or pre-enforcement efforts that would have provided fair notice to party regarding agency's interpretation of internal rules of practice). Administrative adjudications can provide fair notice of the agency's interpretation of the law. *See Otis Elevator Co. v. Secretary of Labor*, 762 F.3d 116, 125 (D.C. Cir. 2014) (noting that administrative adjudication interpreting regulations "is agency action, not a post hoc rationalization of it." (citation and

internal quotation marks omitted)). The Wyndham Appellants do not contend that the FTC's enforcement of its authority to enjoin unfair acts here constitutes "an abrupt change to a longstanding interpretation …." *Id.; see also State of N.Y. v. Shalala*, 119 F.3d 175, 183 (2d Cir. 1997). Indeed, the Wyndham Appellants had fair notice of the sorts of data security practices the FTC would prosecute because the FTC has used its authority to bring enforcement actions against other companies for similar practices *for more than a decade*.

The FTC's data security program began under the direction of then-Chairman Tim Muris, who served as commissioner of the agency from 2000-2004. *The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury: Hearing Before the H. Comm. On Oversight and Gov't Reform*, 113th Cong. 4 (2014) (statement of Woodrow Hartzog, Associate Professor of Law, Samford University's Cumberland School of Law).[15] The FTC settled cases involving conduct similar to Appellants' prior to commencing its investigation of Wyndham. Contrary to the Wyndham Appellants' characterizations, the complaints in those prior cases provide detail about the unfair acts or practices sufficient to place other regulated entities on notice about how to conform their data security practices to the law. In 2005, for example, the FTC settled an

[15] *Available at* http://oversight.house.gov/wp-content/uploads/2014/07/Hartzog-Statement-7-24-FTC.pdf.

enforcement action against BJ's Wholesale Club following allegations that BJ's maintained unfair practices by failing to take reasonable and appropriate security measures to protect the consumer information—including names, credit and debit card numbers, and expiration dates—that it transmitted through its in-store and central computer networks to obtain and receive payment authorizations from issuing banks. FTC Administrative Complaint, Docket No. C-4148, *In the Matter of BJ's Wholesale Club, Inc.*, ¶¶ 4-5, 9-10.[16] Specifically, and similar to the allegations in this case, BJ's failed to encrypt the consumer information it transmitted, allowed anonymous access to the information through the use of default user IDs and passwords, and failed to maintain adequate measures that would detect unauthorized access on its networks. *Id.* at ¶ 7. As a result, hackers were able to obtain consumers' debit and credit card numbers, which were then encoded onto counterfeit cards used to make several million dollars in fraudulent purchases. *Id.* at ¶ 8. Because the card issuers were forced to cancel the cards to prevent further fraudulent use, those consumers were prevented from making purchases using credit or accessing their bank accounts. *Id.* The FTC's settlement with BJ's required the company, among other things, to design and implement a "comprehensive information security program … reasonably designed to protect

[16] *Available at* http://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305comp0423160.pdf.

the security, confidentiality, and integrity of personal information collected from or about consumers," and to retain an independent auditor to certify its compliance with the settlement. FTC Decision and Order, Docket No. C-4148, *In the Matter of BJ's Wholesale Club, Inc.*, at 2-3.[17] These measures offer strong protection for consumer data.

Similarly, the FTC brought an enforcement action in 2006 against CardSystems Solutions, Inc., for failing to take reasonable and appropriate measures to protect customers' credit and debit card information stored on the company's computer network that CardSystems used to process payment authorization requests for card purchases. FTC Administrative Compl., Docket No. C-4168, *In the Matter of CardSystems Solutions, Inc.*, ¶¶ 3, 6.[18] Of particular relevance to this case, the FTC alleged that CardSystems failed to employ an adequate intrusion detection system, failed to employ firewalls or other measures that would have limited access to the payment card information stored on the computer network from the internet, and failed to use strong passwords to protect access to its network that would prevent a hacker from easily guessing what those passwords were. *Id.* at ¶ 6. These failures resulted in a data breach in which

[17] *Available at* http://www.ftc.gov/sites/default/files/documents/cases/2005/09/092305do0423160.pdf.

[18] *Available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/09/0523148cardsystemscomplaint.pdf.

hackers gained access to data for "tens of millions of credit and debit cards." *Id.* at ¶ 7. Some of this information was used to make approximately several million dollars in fraudulent transactions. *Id.* at ¶ 8. The FTC settled its complaint against CardSystems on terms similar to its agreement with BJ's, requiring the implementation and maintenance of a data security system reasonably designed to safeguard consumer information, periodic audits of that system, and retention of documentation of its compliance efforts. FTC Decision and Order at 3-5, Docket No. C-4168, *In the Matter of CardSystems Solutions, Inc. and Solidus Networks, Inc.*[19]

In the FTC's 2008 enforcement action against The TJX Companies, Inc., the FTC alleged that the retailer had engaged in unfair data security acts or practices in violation of Section 5 of the FTC Act. FTC Administrative Compl., Docket No. C-4227, *In the Matter of The TJX Companies, Inc.*, ¶¶ 8, 13.[20] Of particular relevance here, TJX stored consumer information in clear text, did not use a firewall or other common security measures to limit access between the computers storing customer information and the internet, failed to implement security measures to detect and prevent unauthorized access, such as updated antivirus software or investigation of

[19] *Available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/09/0523148cardsystemsdo.pdf.

[20] *Available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxcomplaint.pdf.

security warnings and intrusion alerts, and did not require the use of complex passwords to access its networks and computers. *Id.* at ¶ 8. As a result, TJX's networks were breached on separate occasions in 2005 and 2006. *Id.* at ¶ 9. Information for tens of millions of credit and debit cards was stolen and used to make "tens of millions of dollars in fraudulent charges." *Id.* at ¶ 11. Many customers had their payment cards cancelled and were unable to access credit until replacement cards were issued. *Id.* As with its agreements with BJ's and CardSystems, the FTC's settlement with TJX required the establishment of data security practices aimed at, among other things, the "prevention, detection, and response to attacks, intrusions, or other systems failures" to protect against theft of consumer information. FTC Decision and Order, Docket No. C-4227, *In the Matter of The TJX Companies, Inc.*, at 3.[21]

FTC enforcement actions such as these have provided notice of what constitutes unfair data security practices, and these actions are necessary to address the market failure presented by companies that fail to take reasonable measures to protect consumer data on their systems and to prevent future substantial injury to consumers that is likely to result from a data breach incident.

[21] *Available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxdo.pdf.

CONCLUSION

For the foregoing reasons, the Court should affirm the decision of the district court.

November 12, 2014

Respectfully submitted,

/s/ Jehan A. Patterson
Jehan A. Patterson
D.C. Bar No. 1012119
Scott Michelman
PUBLIC CITIZEN LITIGATION GROUP
1600 20th Street NW
Washington, DC 20009
(202) 588-1000

Attorneys for Amici Curiae
Public Citizen, Inc., et al.,

CERTIFICATION OF BAR MEMBERSHIP

I certify that I am a member of the Bar of this Court.

/s/ Jehan A. Patterson

CERTIFICATION OF SERVICE

I certify that on November 12, 2014, a true and correct copy of the foregoing Brief of Amici Curiae Public Citizen, Inc., et al., was served on all parties to this appeal, via CM/ECF, pursuant to Third Circuit Rule 25.1(b) and L.A.R. Misc. 113.4, because counsel for all parties are Filings Users who will be served electronically by the Notice of Docket Activity.

Joel R. Marcus-Kurn
David C. Shonka
David L. Sieradzki
FEDERAL TRADE COMMISSION
600 Pennsylvania Avenue N.W.
Mail Stop H-584
Washington, DC 20580
Counsel for Appellee

Eugene F. Assaf, P.C.
Christopher Landau, P.C.
Susan M. Davies
K. Winn Allen
KIRKLAND & ELLIS LLP
655 15th Street N.W.
Washington, DC 20005
Counsel for Appellants

Jennifer A. Hradil
Justin T. Quinn
GIBBONS P.C.
One Gateway Center
Newark, NJ 07102
Counsel for Appellants

Michael W. McConnell
STANFORD LAW SCHOOL
559 Nathan Abbott Way
Stanford, CA 04305
Counsel for Appellants

Sean M. Marotta
Catherine E. Stetson
HOGANS LOVELL US
555 13th Street, N.W.
Washington, DC 20005
Counsel for Amici Curiae Chamber of Commerce of the USA, American Hotel & Lodging Association, National Federation of Independent Business

Douglas H. Meal
David T. Cohen
ROPES & GRAY LLP
800 Boylston Street
Boston, MA 02199
Counsel for Appellants

Cory L. Andrews
WASHINGTON LEGAL FOUNDATION
2009 Massachusetts Avenue, N.W.
Washington, DC 20036
Counsel for Proposed Amici Curiae Washington Legal Foundation and Allied Education Foundation

John F. Cooney
VENABLE
575 7th Street, N.W.
Washington, DC 20004
Counsel for Proposed Amicus Curiae Electronic Transactions Association

I certify that on November 12, 2014, I caused to be delivered by first-class mail ten copies of this brief to the Clerk of the Court, as follows:

Marcia M. Waldron, Clerk
U.S. Court of Appeals for the Third Circuit
Room 21400, U.S. Courthouse
601 Market Street
Philadelphia, PA 19106

/s/ Jehan A. Patterson

CERTIFICATION CONCERNING IDENTICAL VERSIONS OF BRIEF

I certify that the electronic and hard copies of this brief are identical.

/s/ Jehan A. Patterson

CERTIFICATION OF COMPLIANCE WITH RULE 32(a)

I certify that this brief complies with Federal Rule of Appellate Procedure 32(a)(7)(B) because this brief contains 4,895 words, excluding those parts of the brief excluded by Fed. R. App. Pro. 32(a)(7)(B)(iii).

/s/ Jehan A. Patterson

CERTIFICATION CONCERNING VIRUS CHECK

I certify that the electronic file of this brief was scanned with VIPRE anti-virus software.

/s/ Jehan A. Patterson