David A. Selden, SBN 007499
The Cavanagh Law Firm, P.A.
1850 North Central Avenue, Suite 2400
Phoenix, Arizona 85004
dselden@cavanaghlaw.com
Phone: (602) 322-4009
Fax: (602) 322-4101

Attorneys for Amici Curiae Chamber of Commerce of the United States of America, Retail Litigation Center, and American Hotel & Lodging Association

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. Wyndham Worldwide Corporation, et al. Defendants.	Case No. CV 12-1365-PHX PGR

LODGED: PROPOSED "BRIEF OF *AMICI CURIAE* CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA, RETAIL LITIGATION CENTER, AND AMERICAN HOTEL & LODGING ASSOCIATION IN SUPPORT OF DEFENDANTS" ATTACHED.

David A. Selden, SBN 007499
The Cavanagh Law Firm, P.A.
1850 North Central Avenue, Suite 2400
Phoenix, Arizona 85004
dselden@cavanaghlaw.com
Phone: (602) 322-4009
Fax: (602) 322-4101

Attorneys for Amici Curiae Chamber of Commerce of the United States of America, Retail Litigation Center, and American Hotel & Lodging Association

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

Federal Trade Commission, Plaintiff, v. Wyndham Worldwide Corporation, et al. Defendants.	Case No. CV 12-1365-PHX PGR **BRIEF OF *AMICI CURIAE* CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA, RETAIL LITIGATION CENTER, AND AMERICAN HOTEL & LODGING ASSOCIATION IN SUPPORT OF DEFENDANTS**

Of Counsel

Catherine E. Stetson
J. Robert Robertson
Harriet P. Pearson
Bret S. Cohen
Hogan Lovells US LLP
555 Thirteenth Street, N.W.
Washington, D.C. 20004
cate.stetson@hoganlovells.com
robby.robertson@hoganlovells.com
harriet.pearson@hoganlovells.com
bret.cohen@hoganlovells.com
Phone: (202) 637-5600
Fax: (202) 637-5910
Counsel for Amici Curiae

Banks Brown
McDermott Will & Emery LLP
340 Madison Ave.
New York, NY 10713
Phone: (212) 547-5488
Fax: (646) 383-6105
Counsel for Amicus Curiae American Hotel & Lodging Association

Deborah R. White
Retail Litigation Center
1700 N. Moore Street, Suite 2250
Arlington, VA 22209
deborah.white@rila.org
Phone: (703) 600-2067
Fax: (703) 841-1184
Counsel for Amicus Curiae Retail Litigation Center

Robin S. Conrad
Sheldon Gilbert
National Chamber Litigation Center, Inc.
1615 H Street, N.W.
Washington, D.C. 20062
RConrad@USChamber.com
SGilbert@USChamber.com
Phone: (202) 463-5337
Fax: (202) 463-5346
Counsel for Amicus Curiae Chamber of Commerce of the United States of America

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES:

STATUTES:

OTHER AUTHORITIES:

BRIEF OF *AMICI CURIAE* CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA, RETAIL LITIGATION CENTER, AND AMERICAN HOTEL & LODGING ASSOCIATION IN SUPPORT OF DEFENDANTS

The Chamber of Commerce of the United States of America (the "Chamber"), the Retail Litigation Center ("RLC"), and the American Hotel & Lodging Association ("AH&LA") submit this brief as *amici curiae* in support of Defendant Wyndham Hotels & Resorts LLC ("Wyndham")'s Motion to Dismiss.

INTEREST OF *AMICI CURIAE*

The Chamber of Commerce of the United States of America is a nonprofit corporation and the world's largest business federation. The Chamber represents 300,000 direct members and indirectly an underlying membership of more than three million companies and professional organizations of every size, in every industry sector, and from every region of the country. The Chamber represents the interests of its members in matters before Congress, the Executive Branch, and the courts. To that end, the Chamber regularly files *amicus curiae* briefs in cases raising issues of vital concern to the nation's business community.

The RLC is a public policy organization that identifies and engages in legal proceedings that affect the retail industry. The RLC's members include many of the country's largest and most innovative retailers. The member entities whose interests the RLC represents employ millions of people throughout the United States, provide goods and services to tens of millions more, and account for tens of billions of dollars in annual sales. The RLC seeks to provide courts with retail-industry perspectives on important legal issues, and to highlight the potential industry-wide consequences of significant pending cases.

The AH&LA is the only national association representing all sectors and stakeholders in the lodging industry, including individual hotel property members, hotel companies, student and faculty members, and industry suppliers. It has played this role for over a century providing members with national advocacy on Capitol Hill, public relations services and education, research, and information.

Electronic data is the pulse of American business. The companies represented by the Chamber, RLC, and AH&LA use electronic data, including personal data, to enhance business efficiency and to benefit consumers. For the modern company, personal and other types of digitized data are essential for a multitude of reasons, including administering employee benefits programs, processing payment and shipping information, and enabling customer loyalty programs, among many other uses. *Amici* all have a significant interest in explaining to the Court the legal and policy implications of accepting the Federal Trade Commission ("FTC" or "Commission")'s arguments, and assisting the Court with resolving the claims pending before it.

INTRODUCTION

The FTC's use of its enforcement authority to regulate "unfair" trade practices under Section 5 of the FTC Act, 15 U.S.C. § 45, has a checkered past. Thirty years ago, the FTC sought to significantly expand the scope of its Section 5 authority, invoking the then-extant version of the statute to advance its consumer protection goals in ways far beyond those envisioned by Congress. Congress reacted to that overreach, codifying into law significant limits on the scope of the FTC's authority.

The FTC has strayed down the same path again. Over the course of the past decade, the FTC has departed from the statutory underpinnings of Section 5 unfairness, leveraging its enforcement authority to extract settlements from businesses that themselves have been victimized by data security breaches, and that have no formal notice of the standards that the FTC accuses them of violating. By statute, the FTC has an important role to play in protecting America's consumers. However, the agency's "unfairness" authority does not permit it to set and enforce – whether through litigation or consent orders[1] – general data-security policy.

[1] Often when the FTC claims that a data-security breach constitutes an "unfair" trade practice, the Commission has been able to obtain Section 5 consent orders from the targeted businesses. This case is among the first data-security "unfairness" proceedings to be evaluated by a court.

Indeed, the FTC expressly has acknowledged that Congress has not granted it the general authority to regulate data security; after all, that is why the Commission currently is lobbying for additional rulemaking authority. The FTC should not be permitted to circumvent the full legislative process by establishing rules and principles through private enforcement actions, resulting in a string of consent orders that the FTC publishes and which it holds out to other businesses as if they were established law.

This incremental – and unilateral – regulation-through-settlement subjects American businesses to vague, unknowable, and constantly changing data-security standards. Companies often are unaware of the standards to which they are held until after they receive a notice of investigation from the FTC, at which point they must settle or expend considerable resources fighting the agency. The *in terrorem* effect of a notice by itself thus is significant. The FTC's arsenal of enforcement capabilities carries a real risk of affecting business judgment, slowing the adoption of new technologies, and chilling business from sharing information about breaches to avert malicious attacks in the future.

Permitting the FTC to proceed on a theory that suffering a data breach is an "unfair" trade practice would expose every business in America to the potential for a government enforcement action whenever that business suffers a cyber-attack or other incident that potentially compromises personal data. Congress did not envision that result when it passed legislation limiting the FTC's Section 5 unfairness authority, and this Court should not countenance it.

The businesses represented by *amici* take seriously their responsibility to safeguard all personally identifying electronic information. But it is a stark reality that bad actors target business technology to obtain valuable data, including personal data and intellectual property. No data security is perfect, and breaches do occur, exposing digital information. But when criminals accessed Wyndham's business computer systems, the FTC sought court redress not against the thieves, but against the business that was

victimized by them, contending in Count II of its complaint that Wyndham's data-security policy was an "unfair," and therefore unlawful, trade practice.

The FTC has overreached. It lacks the legal authority to act as a roving regulator of data security standards, because the statute under which the FTC has purported to act – Section 5 of the FTC Act – does not authorize the Commission to proceed as it has in this case.

Defendant Wyndham's Motion to Dismiss should be granted.

ARGUMENT

I. THE FTC'S SECTION 5 AUTHORITY TO PROHIBIT UNFAIR TRADE PRACTICES DOES NOT GIVE THE FTC AUTHORITY TO ESTABLISH GENERAL DATA SECURITY POLICY.

Defendant Wyndham's Motion to Dismiss [Dkt. #32] explains in detail why the FTC does not have the authority to sanction businesses for data security breaches under Section 5 of the FTC Act. [*See* Dkt. # 32, Wyndham Mot. 6-10]. As Wyndham explains, nothing in Section 5 suggests that Congress intended to give the FTC the authority to regulate data security. Multiple other laws grant the Commission the authority to regulate data security *in certain, limited contexts* – something that would have been entirely unnecessary if Congress already had given the Commission the broad Section 5 authority to regulate data security it now claims it has.[2] Indeed, even the FTC itself does not argue that Congress has expressly authorized the Commission to regulate the data-security practices of private companies. [*See* Dkt. #46, FTC Opp. to Wyndham Mot. 6]. And for good reason: for over a decade, the FTC repeatedly has lobbied for legislation providing it with rulemaking authority under the Administrative Procedure Act (APA) in the area of general data security, thus far to no avail. *See, e.g.*, *Data Security: Hearing Before the H. Comm on Energy & Commerce, Subcomm. on Commerce, Mfg., & Trade*, 112th Cong. 11 (June 15, 2011) (prepared statement of FTC) [hereinafter *FTC 2011 Data*

[2] Congress has explicitly authorized the FTC to oversee and enforce data-security standards for certain industries and situations. [*See, e.g.*, Dkt. # 32, Wyndham Mot. 7-8] (citing FTC's data-security authority under, among other statutes, the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and Children's Online Privacy Protection Act).

Security Testimony][3] (supporting draft legislation that would provide FTC with APA rulemaking authority); FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace* 36-37 (May 2000)[4] (recommending that Congress enact legislation requiring commercial websites to "take reasonable steps to protect the security of the information they collect from consumers" and to "provide an implementing agency with the authority to promulgate more detailed standards pursuant to the Administrative Procedure Act").

The FTC's enforcement actions in fact harken back to past attempts to extend its authority beyond proper bounds – attempts that resulted in Congress's adoption of a statutory test constraining the FTC's unfairness enforcement authority. Congress granted the FTC the authority to prohibit "unfair or deceptive acts or practices" in 1938, but the Commission rarely wielded the "unfairness" aspect of its authority until 1972, when, in dicta, the Supreme Court cited with apparent approval a little-used FTC test for unfairness. J. Howard Beales, III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, 22 J. of Pub. Pol'y & Mktg. 192, 193 (2003) (citing *FTC v. Sperry & Hutchinson Co. (S&H)*, 405 U.S. 233, 244 & n.5 (1972)). Under this old test, the FTC considered three factors when determining whether business conduct was "unfair" to consumers: (1) whether the conduct "offend[ed] public policy"; (2) whether it was "immoral, unethical, oppressive, or unscrupulous"; and (3) whether it "cause[d] substantial injury to consumers." *S&H*, 405 U.S. at 244 n.5 (reversing FTC decision for failure to articulate standards of conduct to address proven consumer injury).

Armed with that Supreme Court dicta, the FTC embarked on an ambitious campaign of using its Section 5 unfairness authority to police business practices that met *any* of these three loose and wide-ranging criteria. In 1978, for example, the Commission issued a report proposing to ban all television advertising to children as "immoral,

---

[3] *Available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf (last visited Oct. 5, 2012).

[4] *Available at* http://www.ftc.gov/reports/ privacy2000/privacy2000.pdf (last visited Oct. 5, 2012).

unscrupulous, and unethical." Beales, 22 J. of Pub. Poly' & Mktg. at 193. Following a series of similar overreaching policy positions, a political backlash ensued, culminating in Congress holding hearings to investigate the FTC's deployment of its unfairness authority. *See* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?* 60 Admin. L. Rev. 127, 137 (2008).

In 1994, Congress adopted 15 U.S.C. § 45(n), which codified a narrower view of the FTC's Section 5 authority first articulated in the wake of the Congressional hearings. Section 45(n) 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* [i] the act or practice causes or is likely to cause substantial injury to consumers [ii] which is not reasonably avoidable by consumers themselves and [iii] 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) (emphasis added).][5]

Despite these acknowledged statutory constraints, carefully calibrated by Congress in response to years of agency overreaching, the FTC again is attempting to use Section 5 inappropriately. The FTC in this case seeks to impose liability on Wyndham for "failure to implement reasonable and appropriate security measures." But liability under Section 5 attaches only when an act *itself* is injurious to consumers. *See FTC v. Neovi, Inc.*, 604 F.3d 1150, 1157 (9th Cir. 2010). So, for example, a business violates Section 5 if it "ha[s] reason to believe" that its actions will cause substantial consumer injury, or when it "facilitate[s] and provide[s] substantial assistance" to a scheme that causes injury.

[5] Section 45(n) of the FTC Act was based in turn on an FTC Policy Statement, *FTC Policy Statement on Unfairness* (Dec. 17, 1980), *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), which sharply departed from the Commission's earlier expansive reading of its unfairness authority. Among other things, the Policy Statement concluded that the third *S&H* factor – consumer injury – was the most important, lessening the ability of the FTC to take public policy concerns, without more, into account when pursuing unfairness enforcement actions. *Id.* at 1073.

See id. at 1156-57.[6] An attack that primarily *victimizes the business itself* cannot be considered "unfair" to consumers.[7] Disregarding these constraints and assigning liability to good corporate citizens for a data-security breach impermissibly stretches the bounds of Section 5.

Instead of following established precedent, the FTC is using its Section 5 unfairness authority to pursue solely its policy prerogatives – something Congress expressly rejected in 15 U.S.C. § 45(n) when it instructed that "public policy considerations may not serve as a primary basis for such determination." Even granting the Commission the best of intentions, it cannot exercise its unfairness authority in a manner inconsistent with its legislative mandate. *See FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 125 (2000).

II. BUSINESSES CANNOT OPERATE EFFECTIVELY AND EFFICIENTLY IN AN "EVOLVING ENFORCEMENT" REGIME.

Unfettered by the statutory restraints on its enforcement authority, the FTC has now begun to exert its will in the data-security area by entering into and publishing a series of consent orders settling charges against businesses under Section 5 for failing to employ what the Commission considers "reasonable and appropriate" measures to protect personal information against unauthorized access. The FTC negotiates, enters into, and publishes most of these agreements before it even files a complaint, subsequently claiming that the data security "standards" it announces in conjunction with the consent orders are legal requirements under Section 5. This piecemeal "regulation by consent order" has enabled the FTC to impose unilaterally its evolving policy choices on

---

[6] For example, the FTC in the past has obtained injunctions under its Section 5 unfairness authority prohibiting defendants from engaging in "phishing" identity-theft scams, through which the defendants sent emails designed to obtain consumers' financial information under false pretenses and used that information to pay for goods or services without the consumers' consent. *See, e.g.*, *FTC v. Hill*, CV No. H-03-5537 (S.D. Tex. May 18, 2004). It is a long, illogical leap for the FTC to equate Wyndham's victimization at the hands of a criminal hacker with a criminal enterprise's phishing scam.

[7] In addition, as Wyndham correctly observes, consumer injury from payment card data theft is "always avoidable and never substantial." [Dkt. #32, Wyndham Mot. 12].

businesses without the oversight of the legislative branch, without participation of the corporate community and other interested stakeholders, and without judicial review. *Cf. Sackett v. EPA*, 132 S. Ct. 1367, 1374 (2012) (rejecting notion that an agency should be permitted to "strong-arm[] . . . parties into 'voluntary compliance' without the opportunity for judicial review").

Regulating in this manner not only inappropriately circumvents the legislative and judicial processes; it also gives *no* advance notice to businesses on what they are required to do to comply with the law in a rapidly changing technological environment. FTC complaints and consent orders premised on businesses not maintaining "reasonable," "appropriate," "adequate," or "proper" data security measures are ambiguous and can (and do) constantly change. Kenneth A. Bamberger & Dierdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247, 291 (2011) ("The reasonableness standard is fluid, evolving, and open to constant reinterpretation."). The FTC, however, rejects the commonsense idea of setting forth "particularized guidelines" for businesses to follow, reasoning that doing so would be impossible because "[d]ata security industry standards are continually changing in response to evolving threats and new vulnerabilities." [Dkt. #46, FTC Opp. to Wyndham Mot. 12]. But it is *precisely because* the appropriate standards are difficult to ascertain that businesses cannot be held to a nebulous notion of "reasonableness," all without any formal guidance before they find themselves in violation of the law.[8]

For example, in many cases, the FTC will announce a violation of Section 5 based on a set of data security practices that, "taken together," allegedly failed to provide reasonable and appropriate security measures. *See, e.g.*, Complaint, *In re Dave &*

[8] The FTC's position is further belied by the fact that in order to accept payment cards from the major card brands, businesses must comply with the strict Payment Card Industry Data Security Standard (PCI DSS) subject to verified compliance audits on an annual basis. *See* PCI Standards Security Council, *Payment Card Industry Security Standards Overview* (2008), https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf (last visited Oct. 5, 2012).

Buster's, FTC File No. 082 3153, at 2 (2010).[9] Where this occurs, it is unclear whether the FTC would consider each of the offending practices to constitute a distinct Section 5 violation, or if not, what combinations of practices the FTC would deem to constitute an unfair practice in the future. And companies have no way of finding out. The absence of clear standards thus enables the Commission to use 20/20 hindsight – "you were breached, therefore your security must have been inadequate" – when evaluating data breaches.

The FTC expressly encourages businesses to follow and adopt the data-security practices announced in its consent orders. *See Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. 9 (July 27, 2010) (prepared statement of FTC)[10] (testimony of FTC Chairman Jon Leibowitz that "[t]he Commission's robust enforcement actions have sent a strong signal to industry about the importance of data security, while providing guidance about how to accomplish this goal"); Lesley Fair, Sr. Staff Att'y, FTC Bureau of Consumer Prot., *Widgets, Whatzits, and Whaddayacallems*, Business Center Blog (Aug. 30, 2011), http://business.ftc.gov/blog/2011/08/widgets-whatzits-and-whaddayacallems (last visited Oct. 5, 2012) (encouraging businesses to interpret its Section 5 fiats broadly: "[S]avvy marketers of widgets pay attention to FTC cases involving whatzits and whaddaycallems . . . it's wise to look at the big picture – and not just at legal developments directly affecting your business."). But discerning any consistent standards from these consent orders is futile because the FTC's definition of what data security principles are "unreasonable" depends on the business it is investigating. Indeed, by the FTC's own admission, it does not issue general data-security rules in part because "industries and businesses have a variety of network structures that store or transfer different types of data, and reasonable network security will reflect the likelihood that such information

[9] *Available at* http://www.ftc.gov/os/caselist/0823153/100608davebusterscmpt.pdf (last visited Oct. 5, 2012).

[10] *Available at* http://www.ftc.gov/os/testimony/ 100727consumerprivacy.pdf (last visited Oct. 5, 2012).

will be targeted and, if so, the likelihood of attack." [*See* Dkt. #46, FTC Opp. to Wyndham Mot. 12]; *see also The Data Security and Breach Notification Act of 2010: Hearing on S. 3742 Before the Subcomm. on Consumer Prot., Prod. Safety, & Ins. of the S. Comm. On Commerce, Sci., & Transp.*, 111th Cong. 7 n.22 (Sept. 22, 2010) (prepared statement of FTC)[11] ("The Commission recognizes that what [data security measures it considers] reasonable . . . will depend on the size and complexity of the business, the nature and scope of its activities, and the sensitivity of the information at issue."). Piecemeal, context-specific consent orders against other businesses cannot provide general guidance.

Complying with consent orders also is onerous. In just about all of its data-security consent orders, the FTC has insisted on periods of supervision of *twenty years*, during which the target company must provide independent audit results and other reports indicating its compliance with the FTC's security principles. *See, e.g.*, Consent Decree and Order for Civil Penalties, Injunction, and Other Relief, *United States v. RockYou, Inc.*, No. 12-CV-1487 (N.D. Cal. Mar. 28, 2012).[12] If the FTC later determines that a company subject to a consent order is not in compliance with a "new" data-security principle, the company is subject to civil penalties of up to $16,000 per violation. *See* 15 U.S.C. § 45(*l*), *as modified by* 16 C.F.R. § 1.98(c). Essentially, a company subject to an FTC consent order can never know if it is compliant with the order until the FTC says it is not.

The FTC does have limited discretion to develop the contours of the unfairness doctrine through the adjudicative process. But courts have long recognized that failure to apply limiting principles to unfairness under Section 5 would permit the FTC "to substitute its own business judgment" for that of companies, *Official Airline Guides, Inc. v. FTC*, 630 F.2d 920, 927 (2d Cir. 1980), and "blur the distinction between guilty and

[11] *Available at* http://www.ftc.gov/os/testimony/100922datasecuritytestimony.pdf (last visited Oct. 5, 2012).

[12] *Available at* http://ftc.gov/os/caselist/1023120/120327rockyouorder.pdf (last visited Oct. 5, 2012).

innocent commercial behavior." *Boise Cascade Corp. v. FTC*, 637 F.2d, 573, 580-82 (9th Cir. 1980). Without well-defined standards for determining whether conduct is "unfair" under Section 5, "the door would be open to arbitrary or capricious administration of § 5," resulting in "a state of complete unpredictability." *E.I. du Pont de Nemours & Co. v. FTC*, 729 F.2d 128, 138-39 (2d Cir. 1984). And it is in this "state of complete unpredictability" that the FTC now operates with substantial, unchecked power, raising significant due process concerns. *See FCC v. FOX Television Stations*, 132 S. Ct. 2307, 2317 (2012) ("A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required.").

The Commission weakly addresses this legal requirement, claiming that its Section 5 data security enforcement against Wyndham "is not moving in a new direction" because it "has been investigating, testifying about, and providing public guidance on companies' data security obligations under the FTC Act for more than a decade." [Dkt. #46, FTC Opp. to Wyndham Mot. 13]. That argument implies that any administrative agency can exercise authority over a subject matter on its own accord simply by making public statements about it. That is not how it works. Administrative agencies are permitted to act only with, and within, the authorization of Congress. Importuning Congress to permit them to act is not the same.

The FTC's recent attempt to regulate by consent order likewise contradicts U.S. Supreme Court precedent and the FTC's own opinions. *See Altria Group, Inc. v. Good*, 555 U.S. 70, 89 n.13 (2008) (stating that an FTC "consent order is in any event only binding on the parties to the agreement"); *United States v. E. I. du Pont de Nemours & Co.*, 366 U.S. 316, 330 n.12 (1961) ("The circumstances surrounding . . . negotiated [consent orders] are so different that they cannot be persuasively cited in a litigation context."); *In re Chrysler Corp.*, 87 F.T.C. 719, 742 n.12 (1976) (ALJ decision 1975, adopted as modified by full Commission 1976); *see also In re Trans Union Corp.*, 118 F.T.C. 821, 864 n.18 (1994) (noting that a "consent agreement [with one party] is binding

only between the Commission and [that party]"). Congress also emphasized the uniqueness of consent orders in its revision to the FTC Act by excluding them as precedent for "civil penalties." 15 U.S.C. § 45(m)(1)(B). It is thus inappropriate for the FTC to use consent orders to establish industry-wide standards.

III. DATA SECURITY POLICY CANNOT BE DEVELOPED THROUGH UNILATERAL PRONOUNCEMENT BY THE FTC, WITHOUT REGARD FOR THE LEGISLATIVE PROCESS.

Last year, the Commission entered into consent orders with three resellers of credit reports for allegedly "unreasonable" data security measures. *See* Press Release, FTC, *Credit Report Resellers Settle FTC Charges; Security Failures Allowed Hackers to Access Consumers' Personal Information* (Feb. 3, 2011).[13] These were the first-ever Section 5 data-security enforcement actions in which the FTC held a company responsible for its *users'* data-security failures. Four FTC Commissioners acknowledged that fact in a rare statement issued along with the consent orders:

> [W]e are also cognizant of the fact that these are the first cases in which the Commission has held resellers responsible for downstream data protection failures. Looking forward, the actions we announce today should put resellers – indeed, all of those in the chain of handling consumer data – on notice of the seriousness with which we view their legal obligations to proactively protect consumers' data. The Commission should use all of the tools at its disposal to protect consumers from the enormous risks posed by security breaches that may lead to identity theft.

Revised Statement of Commissioner Brill, In Which Chairman Leibowitz and Commissioners Rosch and Ramirez Join, *In re Settlement One Credit Corp., ACRAnet, Inc., and Fajilan & Assocs.*, FTC File Nos. 082 3208, 098 3088, 092 3089 (Aug. 15, 2011).[14] This statement is emblematic of the FTC's "shoot first, ask questions later" ad-hoc approach to regulating data security, with the Commission admitting that it enforces standards against businesses *without any prior notice*. The FTC may have thought that it was being magnanimous to *future* businesses by informing them of the standard "[l]ooking forward"; in reality, it was holding the respondents in this case responsible to

---

[13] *Available at* http://www.ftc.gov/opa/2011/02/settlement.shtm (last visited Oct. 5, 2012).

[14] *Available at* http://www.ftc.gov/os/2011/08/ 110819settlementonestatement.pdf (last visited Oct. 5, 2012).

a standard that they did not know existed. And that will happen each and every time the FTC enforces a new element of its evolving data-security policy.

There is, of course, a *right* way to establish consistent and transparent data-security standards: through a dialogue with all involved stakeholders, accomplished through democratically accountable means, not just by agency fiat. At the same time the Commission is wielding "all of the tools at its disposal" – and then some – to enforce its own data-security prerogatives against individual companies, policymakers, businesses, consumer advocacy groups, and other interested entities – including *amici* – are engaging in a serious debate over how to craft data security policy in the United States. The dialogue among these many groups, including the Chamber and the Commission, includes not only the protection of consumer information but also the overall functioning of the nation's digitally enabled critical infrastructures. *See generally* Joint Ass'n Letter to Senate Regarding Amendments to S. 3414 (July 27, 2012)[15] (advocating for delay in consideration of "vitally important" data security bill because "work is still needed as disagreement persists regarding certain provisions of a federal bill"); Cong. Res. Serv., *Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions* (June 29, 2012)[16] (analyzing proposed cybersecurity legislation); *FTC 2011 Data Security Testimony* (advocating for data security legislation). As Wyndham points out, a number of bills were introduced in Congress in 2011 and 2012, including bills that would have given the FTC rulemaking authority over general data security. None were enacted. [*See* Dkt. #32, Wyndham Mot. 8-9]. Instead of focusing its policy efforts on Congress, however, the FTC has engaged in backdoor rulemaking through its consent orders without having to answer to Congress or the courts.

---

[15] *Available at* http://www.uschamber.com/sites/default/files/hill-letters/Joint%20Association%20Letter%20re%20Amdts%20to%20S%203414.pdf (last visited Oct. 5, 2012).

[16] *Available at* https://www.fas.org/sgp/crs/natsec/R42114.pdf (last visited Oct. 5, 2012).

The FTC failed to effectuate its policy goals through Section 18 rulemaking. Under Section 18 of the FTC Act, the Commission is authorized to prescribe "rules which define with specificity acts or practices which are unfair" in violation of Section 5. 15 U.S.C. § 57a. By Congressional design, this rulemaking authority is more burdensome on the FTC than rulemaking authority normally provided to administrative agencies under the APA; among other restrictions, for example, the statute permits interested parties to cross-examine witnesses. But the FTC has *never attempted to issue data-security rules in this manner*. Instead, the Commission has eschewed this rulemaking procedure as too cumbersome to promulgate data-security rules, instead advocating for less-burdensome rulemaking authority under the APA. *See FTC 2011 Data Security Testimony* at 11 (supporting provision in draft legislation granting APA rulemaking authority to FTC in lieu of Section 18 rulemaking authority because "effective consumer protection requires that the Commission be able to promulgate these rules in a more timely and efficient manner"). Issuing prescriptive data-security requirements outside of the context of these established rulemaking procedures further demonstrates that the FTC is not interested in pursuing constitutionally and legislatively required channels, in line with how it proceeded over thirty years ago.

By sidestepping both the legislative and authorized administrative methods for advancing its policy goals, the FTC is in violation of its Congressional mandate. Instead of respecting the legislative process and the proper means for seeking and receiving express authority to regulate in the general data-security space, the FTC, much as it did in the late 1970s, has breached the boundaries of its Section 5 unfairness authority by engaging improperly in *ultra vires* regulation by consent order.

* * *

Amici acknowledge the importance of data security and, more broadly, cybersecurity, in today's digitally connected world. Businesses have every incentive to move to protect their digital assets in this dynamic technological environment. And government has an important role to play as well, both in protecting governmental

operation and in partnering with industry to provide fair, transparent, and consistent legal frameworks that companies can efficiently assess and apply in a rapidly changing environment.

The FTC historically has had an important, statutorily mandated role to play in protecting consumers. But its attempt to expand its current unfairness enforcement power to the technically complex and dynamic risk-management practices of businesses in almost every sector has stretched its statutory authority beyond the breaking point.

CONCLUSION

For these reasons, and for those stated in Wyndham's Motion to Dismiss, the Motion should be granted.

RESPECTFULLY SUBMITTED this 5th day of October, 2012.

THE CAVANAGH LAW FIRM, P.A.

By: s/David A. Selden

David A. Selden
1850 North Central Avenue, Suite 2400
Phoenix, AZ 85004
dselden@cavanaghlaw.com
Phone: (602) 322-4009
Fax: (602) 322-4101
Attorneys for Amici Curiae

Of Counsel:

Catherine E. Stetson
J. Robert Robertson
Harriet P. Pearson
Bret S. Cohen
Hogan Lovells US LLP
555 Thirteenth Street, N.W.
Washington, D.C. 20004
cate.stetson@hoganlovells.com
robby.robertson@hoganlovells.com
harriet.pearson@hoganlovells.com
bret.cohen@hoganlovells.com
Phone: (202) 637-5600
Fax: (202) 637-5910
Counsel for Amici Curiae

Robin S. Conrad
Sheldon Gilbert
Chamber of Commerce of the
United States of America
1615 H Street, N.W.
Washington, D.C. 20062
RConrad@USChamber.com
SGilbert@USChamber.com
Phone: (202) 463-5337
Fax: (202) 463-5346
Counsel for Amicus Curiae Chamber of Commerce of the United States of America

Deborah R. White
Retail Litigation Center
1700 N. Moore Street, Suite 2250
Arlington, VA 22209
deborah.white@rila.org
Phone: (703) 600-2067
Fax: (703) 841-1184
Counsel for Amicus Curiae Retail Litigation Center

Banks Brown
McDermott Will & Emery LLP
340 Madison Ave.
New York, NY 10713
Phone: (212) 547-5488
Fax: (646) 383-6105
Counsel for Amicus Curiae American Hotel & Lodging Association

CERTIFICATE OF SERVICE

I hereby certify that on October 5, 2012, I electronically transmitted the attached document to the Clerk's Office using the CM/ECF System for filing and transmittal of a Notice of Electronic Filing to the following CM/ECF registrants:

Andrea Vanina Arias
aarias@ftc.gov
John Andrew Krebs
jkrebs@ftc.gov
Jonathan Eli Zimmerman
jzimmerman1@ftc.gov
Katherine E. McCarron
kmccarron@ftc.gov
Kevin H. Moriarty
kmoriarty@ftc.gov
Kristin Krause Cohen
kcohen@ftc.gov
Lisa Naomi Weintraub Schifferle
lschifferle@ftc.gov
Federal Trade Commission - Washington, DC
600 Pennsylvania Ave. NW
Washington, DC 20580
Attorneys for Plaintiff

David B. Rosenbaum
drosenbaum@omlaw.com
Anne M. Chapman
achapman@omlaw.com
Osborn Maledon, P.A.
2929 North Central Avenue, Suite 2100
Phoenix, Arizona 85012-2794
Attorneys for Defendants

Eugene F. Assaf, P.C. (*Pro Hac Vice*)
eugene.assaf@kirkland.com
K. Winn Allen, 1000590 (*Pro Hac Vice*)
winn.allen@kirkland.com
Kirkland & Ellis LLP
655 Fifteenth Street, N.W.
Washington, D.C. 20005
Attorneys for Defendants

Douglas H. Meal (*Pro Hac Vice*)
douglas.meal@ropesgray.com
Ropes & Gray, LLP
Prudential Tower
800 Boylston Street
Boston, MA 02199-3600
Attorneys for Defendants

s/Michele Maul