Stephen M. Orlofsky, Esquire
New Jersey Resident Partner
Rachel J. Gallagher, Esquire
BLANK ROME LLP
301 Carnegie Center, 3rd Floor
Princeton, NJ 08540
Telephone: (609) 750-7700
Fax: (609) 750-7701
Orlofsky@BlankRome.com
RGallagher@BlankRome.com

Attorneys for Amici Curiae TechFreedom, International Center for Law and Economics & Consumer Protection Scholars Justin ("Gus") Hurwitz, Esquire, Todd J. Zywicki, Esquire, and Paul H. Rubin, Ph.D

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

FEDERAL TRADE COMMISSION, Plaintiff, v. WYNDHAM WORLDWIDE CORPORATION, ET AL., Defendants.	Civil Action No. 2:13-cv-01887(ES)(SCM) **AMICI CURIAE BRIEF OF TECHFREEDOM, INTERNATIONAL CENTER FOR LAW AND ECONOMICS & CONSUMER PROTECTION SCHOLARS** Return Date: June 17, 2013

OF COUNSEL & ON THE BRIEF

Berin Szoka, Esquire
TechFreedom
Counsel for TechFreedom

Geoffrey A. Manne, Esquire
International Center for Law and Economics
Counsel for the International Center for Law and Economics

TABLE OF CONTENTS

Page Nos.

TABLE OF AUTHORITIES

Page Nos.

CASES

STATUTES

OTHER AUTHORITIES

BRIEF OF *AMICI CURIAE*

TechFreedom, the International Center for Law & Economics, Justin ("Gus") Hurwitz, Esquire, Todd J. Zywicki, Esquire, and Paul H. Rubin, Ph.D submit this brief as *amici curiae* in support of Defendant, Wyndham Hotels & Resorts, LLC (Wyndham)'s Motion to Dismiss.[1]

INTEREST OF *AMICI CURIAE*

TechFreedom is a nonprofit, nonpartisan public policy think tank. It encourages development of "simple rules for a complex world" across a wide range of information technology policy issues, including privacy, data security, and antitrust.

The International Center for Law & Economics is a nonprofit, non-partisan global research and policy center specializing in regulatory law and economics. ICLE's scholars and scholarship builds the intellectual foundation for rigorous, economically-grounded, evidence-based policy.

Justin ("Gus") Hurwitz, Esquire is a Fellow at the Center for Technology, Innovation, and Competition at the University of Pennsylvania Law School. His

[1] The remaining Wyndham Defendants filed a separate Motion to Dismiss, relying on Wyndham Hotels & Resorts, LLC's brief. Thus, while this brief further develops arguments raised in Defendant, Wyndham Hotels & Resorts, LLC's Motion to Dismiss, this brief is filed in support of all "Wyndham Defendants" – collectively, Wyndham Worldwide Corporation, Wyndham Hotel Group, LLC, Wyndham Hotels and Resorts, LLC and Wyndham Hotel Management, Inc – and both pending Motions to Dismiss before the Court.

expertise includes antitrust, telecommunications and internet law, regulatory law and economics, and law and technology.

Todd J. Zywicki, Esquire is a Foundation Professor of Law at George Mason University School of Law. Professor Zywicki served as the Director of the Office of Policy Planning at the Federal Trade Commission ("FTC").

Paul H. Rubin, Ph.D is the Samuel Candler Dobbs Professor of Economics at Emory University. From 1983-1985 he was Assistant Director of the Bureau of Economics for Consumer Protection at the FTC.

INTRODUCTION

The power to determine whether the practices of almost any American business are "unfair" makes the Federal Trade Commission (FTC) uniquely powerful.[2] This power allows the FTC to protect consumers from truly harmful business practices not covered by the FTC's general deception authority. But without effective enforcement of clear limiting principles, this power may be stretched beyond what Congress intended.

In 1964, the Commission began using its unfairness power to ban business practices that it determined offended "public policy." Emboldened by vague Supreme Court dicta comparing the agency to a "court of equity," *FTC v. Sperry &*

[2] We do not address Wyndham's argument that subsequent legislation authorizing the FTC to implement data security regulation in certain areas precludes general application of Section 5 to data security. *See* WHR Mot. to Dismiss at 7-14.

Hutchinson Co., 405 U.S. 233, 244 (1972), the Commission set upon a series of rulemakings and enforcement actions so sweeping that the Washington Post dubbed the agency the "National Nanny."[3] The FTC's actions eventually prompted Congress to briefly shut down the agency to reinforce the point that it had not intended the agency to operate with such expansive authority. The FTC survived as an institution only because, in 1980, it (unanimously) issued a Policy Statement on Unfairness laying out basic limiting principles to constrain its power and assuring Congress that these principles would be further developed over time:

> Unjustified consumer injury is the primary focus of the FTC Act . . . . The independent nature of the consumer injury criterion does not mean that every consumer injury is legally "unfair," however. To justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided. *In re International Harvester Co*., 104 F.T.C. 949, 1072 (1984) (emphasis added)
>
> [hereinafter, "Unfairness Statement"].

Congress codified the essence of this statement in Section 5 of the Federal Trade Commission Act ("Section 5") in 1994. 15 U.S.C. § 45(n) (2012). And for a time, the Commission used its unfairness power sparingly and carefully, largely out of fear of reawakening Congressional furor.

---

[3] Wash. Post, March 1, 1978 (*cited in* J. Howard Beales, III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, § III, http://www.ftc.gov/speeches/beales/unfair0603.shtm).

But in the last nine years, the unfairness power has risen again as the Commission has increasingly grappled with consumer protection questions raised by the accelerating pace of technological change brought by the Digital Revolution. Today, unfairness is back—but without the limiting principles that Congress agreed were essential to properly restraining the FTC's power.

In 1980, the FTC itself declared that "The task of identifying unfair trade practices was therefore assigned to the Commission, ***subject to judicial review***, in the expectation that the underlying criteria would evolve and develop over time." *Unfairness Statement*, 104 F.T.C. at 1073. Today, these criteria remain little more than vague abstractions, with little analytical rigor. The FTC has brought forty-one data security cases, with seventeen premised on unfairness, and increasingly tacks unfairness claims onto deception claims in a wide variety of cases involving emerging technologies. Yet we know little more today than we did in 1980 about how the FTC analyzes each prong of Section 5. We know even less about how the FTC assesses unfairness in the data security context because the agency has issued no relevant rules or regulations and because the FTC has resolved all its prior actions through consent decrees, not litigation on the merits. This leaves businesses unable to predict what the FTC might deem unfair—the essence of the rule of law.

Since the problem is a lack of judicial adjudication, it might seem counter-intuitive that the court should dismiss the FTC's suit on the pleadings. But this is

precisely the form of adjudication required: The FTC needs to be told that its complaints do not meet the minimum standards required to establish a violation of Section 5 because otherwise there is little reason to think that the FTC's complaints will not continue to be the Commission's primary means of building law (what amounts to "non-law law"). But even if the FTC re-files its unadjudicated complaint to explain its analysis of the prongs of the Unfairness Doctrine, it will not have solved yet another fundamental problem: its failure to provide Wyndham with sufficient guidance *ex ante* as to what "reasonable" data security practices would be.

Denying the motion to dismiss will vindicate the FTC's enforcement of Section 5 through poorly plead complaints that fail to satisfy the statutory requirements for the FTC's use of is unfairness authority. The questions raised below are not questions about the adequacy of Wyndham's data security practices in particular, or even whether they could conceivably be declared unfair upon a full analysis of the facts and proper development of limiting principles. Instead, this brief speaks to the fundamental problems of vagueness and due process raised by the FTC's routine enforcement actions *prior to* adjudication by any court.

First, we believe that it falls to the courts to demand that the FTC develop the law of data security through rulemakings, and other forms of guidance to give companies advance notice of how unfairness applies to them. A ruling that the

FTC's enforcement of Section 5 is vague as applied to Wyndham would be a catalyst for such a change in the FTC's approach. Second, we believe that the Court should require the FTC to plead claims with enough factual development to satisfy the general requirement of plausibility. The current model of using conclusory allegations to pressure companies to settle cannot continue without further endangering the rule of law and leaving the Commission free to continue deciding the bounds of its own authority. Ultimately, the Commission bears a heavy burden of establishing all three elements of unfairness. If the FTC cannot establish its burden in a case such as this, the Court can help protect consumers by clearly stating that it is up to Congress, not the FTC, to decide how to protect consumers against harms that the Unfairness Doctrine cannot properly reach.

ARGUMENT

I. THE SECTION 5 UNFAIRNESS CLAIM IS UNCONSTITUTIONALLY VAGUE AS APPLIED TO WYNDHAM'S DATA SECURITY PRACTICES.

The FTC has charged *seventeen* companies with conducting unfair trade practices for failing to have "reasonable data security." Remarkably, every single company before Wyndham has settled. Thus, the FTC has not developed the basic analysis of unfairness as applied to data security through its enforcement actions, and the FTC has declined to use its general rulemaking power under Section 5 to do so; the FTC has not issued any guidance as to what would constitute reasonable

data security practices. But *some* guidance is required, and the Unfairness Policy Statement cannot on its own, or combined with a pseudo-common law of unadjudicated settlements lacking any doctrinal analysis, provide sufficient grounds to separate the fair from the unfair.

Our legal system rests on the fundamental principle that laws "must give fair notice of conduct that is forbidden or required." *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012). The "void for vagueness" doctrine protects two Due Process concerns: (1) rules must be clear enough to give "give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly"; and (2) precision and guidance are necessary so that enforcers of the law do not act arbitrarily or discriminatorily. *Id.*; *see also Grayned v. City of Rockford*, 408 U.S. 104, 108-09 (1972). While economic regulations are typically subject to a less stringent vagueness analysis than those burdening speech, factors such as legal and reputational consequences can trigger a more demanding Due Process analysis. *Cf. FCC v. Fox*, 132 S. Ct. at 2318-19; *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498-90 (1982).

The FTC's current approach to data security denies companies like Wyndham "a reasonable opportunity to know what is prohibited" and thus follow the law. The FTC has previously suggested that its Congressional testimony offers all the "public" guidance a company would need. *See* 10/2/2012 FTC Opp. to

Wyndham Mot. (D.I. 45) 7, 13; *see also Identity Theft: Innovative Solutions for an Evolving Problem: Hearing Before the Subcomm. on Terrorism, Tech., & Homeland Sec. of the S. Comm. on the Judiciary*, 110th Cong. 91-94 (2007) (statement of Lydia Parnes, Director of Bureau of Consumer Protection, FTC). But collectively this testimony merely summarizes past the consent decrees, which add no meaningful analysis of limiting principles to the complaints themselves, which are inadequate for the reasons explained below. *See infra* Sec. II. Settlements (and testimony summarizing them) do not in any way constrain the FTC's subsequent enforcement decisions; they cannot alone be the basis by which the FTC provides guidance on its unfairness authority because, unlike published guidelines, they do not purport to lay out general enforcement principles and are not recognized as doing so by courts and the business community. *See, e.g., United States v. Syufy Enterprises*, 903 F.2d 659 (9th Cir. 1990) (deciding against the DOJ in part on the grounds that it did not adhere to the Horizontal Merger Guidelines). It is impossible to imagine a court faulting the FTC for failure to adhere to a previous settlement, particularly because settlements are not readily generalizable and bind only the parties who agree to them. *See, e.g.*, *Altria Group, Inc. v. Good*, 555 U.S. 70, 89 n. 13 (2008) (noting a FTC "consent order is... only binding on the parties to the agreement"). Even setting aside this basic legal principle, the gradual accretion of these unadjudicated settlements does not solve the vagueness problem: While

guidelines provide cumulative analysis of previous enforcement decisions to establish general principles, these settlements are devoid of doctrinal analysis and offer little more than an infinite regress of unadjudicated assertions.

Rulemaking is generally preferable to case-by-case adjudication as a way to develop agency-enforced law, because rulemaking both reduces vagueness and constrains the mischief that unconstrained agency actions may cause—the two concerns raised in *Grayned*. *See SEC v. Chenery Corp.*, 332 U.S. 194, 202 (1947) ("The function of filling in the interstices of [a statute] should be performed, as much as possible, through this quasi-legislative promulgation of rules to be applied in the future."). It may, indeed, not be possible to "draft[ ] a complete list of unfair [data security] practices that would not quickly become outdated or leave loopholes for easy evasion." *Unfairness Statement*, 104 F.T.C. at 1073. Those aspects of data security that cannot easily be reduced to rules might well be more amenable to case-by-case adjudication. But without Article III court decisions developing binding legal principles and no other meaningful form of guidance from the FTC, the law will remain unconstitutionally vague. The FTC's approach to enforcement also allows the FTC to act both arbitrarily and discriminatorily. *Grayned*, 408 U.S. at 108. The FTC today can coerce companies into changing their business practices and impose a 20-year consent decree with regular audits. Courts enforce violations of consent decrees under what amounts to a strict

liability standard through its contempt power. *See* 18 U.S.C. §§ 401-02. Violations carry not only harsh penalties,[4] but also significant reputational consequences. This power violates the due process rights of companies targeted by the FTC, including Wyndham.

Burdensome as settlements can be, *not* settling can be even costlier. Wyndham, for example, has already received 47 document requests in this case and spent $5 million responding to these requests. Motion to Stay Discovery at 5. The FTC's compulsory investigative discovery process and administrative litigation both consume the most valuable resource of any firm: the time and attention of management and key personnel. All this occurs before the FTC has explained the nature of the alleged violation and without effective judicial oversight. Unlike the normal discovery process in civil litigation, the FTC's civil investigative demand ("CID") process offers investigation targets few, if any, due process rights, such as the right to appear at a hearing. It is secretive and informal. *See generally* 15 U.S.C. § 57b-1. If the business refuses to settle, the FTC can simply drag out the process further, racking up legal expenses for the target that are so burdensome that few companies will find it worth pursuing whatever minimal due process rights they have in the CID process. Thus has the FTC been able build

[4] *See, e.g.*, Statement of FTC, *In the Matter of Google Inc*., FTC No. C-4336 (imposing $22.5 million fine for violation of Google Buzz settlement).

this line of data security enforcement actions for nine years without facing an Article III court.

This dynamic is, of course, the result of the low bar the Supreme Court set for administrative subpoenas in *United States v. Powell*. But even there, the Court cautioned against the potential for abuse of subpoenas that may "harass the taxpayer or... put pressure on him to settle a collateral dispute…" 379 U.S. 48, 58 (1964). Deliberate or not, the line of forty-one data security settlements suggests that this is what the FTC has done here. Such a strategy is questionable to begin with, but it is more problematic where, as here, the result is that the FTC has developed a non-binding "common-law of settlements"—a term used proudly by one FTC Commissioner.[5] This has "collateral" effects on future investigations, and robs businesses of the notice required by due process. *Powell*, 379 U.S. at 58, *Fox II*, 132 S. Ct. at 2317. This strategy is also problematic under *Chenery II*, which expressly notes a preference for the development of rules of general applicability, because the agency's strategy forecloses the development of such rules.

Additionally, the FTC can always insist on prosecuting a recalcitrant company through its internal "Part III" adjudicative processes. The target

[5] Julie Brill, FTC Commissioner, *Privacy, Consumer Protection, and Competition* (Apr. 27, 2012), *available at* http://www.ftc.gov/speeches/brill/120427loyolasymposium.pdf.

company could spend months in administrative litigation before ever reaching an independent Article III tribunal. *See* 16 C.F.R. Part 3. This means the company faces two practically certain defeats—before the administrative law judge and then the full Commission, each a public relations disaster. The FTC appears to be perfectly willing to use negative media to encourage settlements: The House Oversight Committee is currently investigating whether a series of leaks by FTC staff to media last year were intended to pressure Google to settle the FTC's antitrust investigation[6] into the company's business practices.[7]

A target company can always "do it the easy way" and avoid these pressures, with the FTC imposing a consent decree (but no monetary penalty, *see* 15 U.S.C. § 45(l) (2012)), other than, potentially and as the FTC seeks here, disgorgement), and publishing a single press release that does relatively little reputational damage.

II. THIS COURT SHOULD ESTABLISH PLEADING STANDARDS FOR DATA SECURITY CASES UNDER SECTION 5.

The FTC's Amended Complaint ("Complaint") provides so little factual content that its unfairness claim should be dismissed under FRCP 8(a), which

[6] Statement of the FTC Regarding Google's Search Practices, *In the Matter of Google Inc.*, FTC File Number 111-0163, Jan. 3, 2013, *available at* http://www.ftc.gov/os/2013/01/130103googlesearchstmtofcomm.pdf.

[7] *See, e.g.*, Timothy B. Lee, *Congressman calls for investigation of leaks in Google antitrust case*, ARSTECHNICA, Jan. 7, 2013, http://arstechnica.com/tech-policy/2013/01/congressman-calls-for-investigation-of-leaks-in-google-antitrust-case/.

requires enough facts to state a plausible claim for relief. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). If the court determines the Complaint's deception claim provides sufficient factual content to survive the motion to dismiss, the court should clarify that such a claim falls under the heightened particularity standard of FRCP 9(b) because it "sounds in fraud." *See, e.g.*, *FTC v. Lights of Am., Inc.*, 760 F.Supp.2d 848, 853 (C.D. Cal. 2010); *FTC v. Ivy Capital, Inc.*, 2011 WL 2118626, at *3 (D. Nev. May 25, 2011).

A. COUNT II FAILS TO ALLEGE FACTS SUPPORTING EACH STATUTORILY REQUIRED ELEMENT OF AN UNFAIRNESS CLAIM.

Under Section 5, a practice can be found unfair only if it "causes or is likely to cause *substantial injury to consumers* which is *not reasonably avoidable* by consumers themselves and not outweighed by *countervailing benefits* to consumers or to competition" 15 U.S.C. § 45(n) (2012) (emphasis added). The FTC's unfairness claim lacks the requisite facts to plausibly satisfy these three prongs. FRCP 8 exists to ensure that "a plaintiff with 'a largely groundless claim' [may not] 'take up the time of a number of other people'" or use the threat of costly litigation as leverage to force a defendant into settling. *Twombly*, 550 U.S. at 557-58. A claim is facially plausible when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. *Iqbal*, 556 U.S. at 678. Assuming the facts are true, there must

be enough present in the complaint to raise the allegation above speculation. *Twombly*, 550 U.S. at 555. While legal conclusions can provide the framework of a complaint, "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678.

1. Substantial Injury

"Unjustified consumer injury is the primary focus of the FTC Act." *Unfairness Statement*, 104 F.T.C. at 1073. In deception cases, injury can be presumed so long as the representation, omission or practice is "material" to the consumer's choices about the product or service.[8] But in unfairness cases, the FTC bears the burden of establishing injury. The Complaint falls far short of establishing that *consumers* suffered substantial injury here. The Complaint does even not make clear what the FTC believes constitutes the substantial injury. Many of the vague assertions on which the FTC's claim of substantial injury seems to rely would expand this essential element—"the primary focus of the FTC Act"—far beyond what the FTC itself contemplated in the Unfairness Policy Statement.

As the FTC itself has said, "The Commission is not concerned with trivial or merely speculative harms. In most cases a substantial injury involves monetary harm.... Emotional impact and other more subjective types of harm, on the other

[8] *In re Cliffdale Associates, Inc.*, 103 F.T.C. 110, 166 (1984) [hereinafter, "Deception Statement").

hand, will not ordinarily make a practice unfair." *Unfairness Statement*, 104 F.T.C. at 1073. Thus, the best reading of 15 U.S.C. § 45(n) is that "substantial injury" generally refers to concrete economic harms, such as unreimbursed account charges to consumers. Where the FTC would rest unfairness charges on less objective, quantifiable harms, it should bear a correspondingly heavy burden of defining the harm. As Howard Beales, former director of the FTC's Bureau of Consumer Protection, has put it: "the Commission should not be in the business of trying to second guess market outcomes...when the existence of consumer injury is itself disputed. That's the point of the substantial injury test."[9]

The FTC simply has not met that burden. They allege that bad actors were able to access credit card data and place "fraudulent charges on many consumers' accounts," causing "more than $10.6 million in fraud loss." Am. Compl. § 24. But these allegations do not establish a plausible substantial injury to consumers under Section 5. It is unclear under the alleged facts whether *consumers* suffered more than a "trivial" harm, as federal law places a $50 limit on what consumers can be charged for unauthorized use of a payment card. 15 U.S.C. § 1643(a)(1)(B) (2012).

Here, the FTC has failed to allege any cognizable injury beyond the vague assertion of unreimbursed charges, obscuring a vital distinction: whether the "$10.6 million in fraudulent charges" refers to unreimbursed charges (borne by

[9] Beales, *supra* note 2.

consumers) or reimbursed charges (borne by businesses). Former FTC Chairmen Majoras and Kovacic voiced this concern, dissenting in *N-Data*, that the Commission was inappropriately extending *consumer* protection law to sophisticated corporations.[10]

Similarly, courts considering data security claims under state law have required more than emotional injury, relatively minor financial losses, or the risk of future injury. *See, e.g.*, *Reilly v. Ceridian Corp.*, 664 F.3d 38, 44-45 (3d Cir. 2011). Damages due to the costs associated with the increased risk of identity theft, including the present and future costs of mitigation such as credit monitoring services, are normally rejected as an injury independent from actual monetary or property loss. *See id.* at 46; *Randolph v. ING Life Ins. & Annuity Co.*, 486 F.Supp.2d 1, 8 (D.D.C. 2007) ("[T]he 'lost data' cases . . . clearly reject the theory that a plaintiff is entitled to reimbursement for credit monitoring services or for time and money spent monitoring his or her credit."). Other economic harms, like the loss of accumulated reward points, are similarly too attenuated and thus speculative. Reimbursed charges have also been rejected as an injury, since they represent no actual loss. *See Hammond v. The Bank of New York Mellon Corp.*,

[10] Majoras Dissent, N-Data, *available at* http://www.ftc.gov/os/caselist/0510094/080122majoras.pdf ("[T]he FTC has used its authority under Section 5 to protect small businesses against unfair acts and practices.... There is a clear qualitative difference between these entities and...computer manufacturers").

2010 WL 2643307, at *8 (S.D.N.Y. June 25, 2010); *Randolph*, 486 F. Supp. 2d at 8.

2. Reasonably Avoidable

The FTC provides no factual support whatsoever for the allegation that consumers could not have reasonably avoided whatever injury they might have suffered. 15 U.S.C. § 45(n). The FTC simply concludes that the injury was not reasonably avoidable in the description of the FTC Act and the conclusion in Count II. *See* Am. Compl. ¶¶ 43, 48. This is exactly the sort of "[t]hreadbare recital[] of the elements of a cause of action, supported by mere conclusory statements" the Supreme Court has deemed inadequate. *Iqbal*, 556 U.S. at 678.

In particular, the FTC fails to support the allegation that "unreimbursed fraudulent charges" are not reasonably avoidable by consumers. In fact, consumers could do so by putting a hold on the credit card, requesting a new card number, purchasing credit monitoring services, or by notifying the card issuer of unauthorized charges. The FTC asserts that "consumers and businesses... expended time and money resolving fraudulent charges and mitigating subsequent harm" but fails to provide any facts to permit a "reasonable inference" (as required by *Iqbal*) that these costs were *unreasonable*. Indeed, the only reasonable inference that can be drawn from the FTC's factual allegations is that *any* effort spent avoiding injury is not "reasonable"—a claim which would negate one prong of analysis required

by Section 5. The FTC must plead additional facts to support a reasonable inference as to the level at which avoidance costs are sufficient to meet the requirement of Section 5. Even if it could properly extend to injuries suffered by large companies like credit card issuers, they can already reasonably avoid injury by, for example, imposing their own data security requirements on vendors by contract. The Unfairness Doctrine ought not supplant such private ordering.

3. Countervailing Benefits

The FTC says nothing to establish even a plausible allegation that there were no "countervailing benefits" to the business practices at issue. *See* Am. Compl. ¶¶ 43, 48. Instead, the FTC's allegation is exactly the sort of "[t]hreadbare recital[] of the elements of a cause of action, supported by mere conclusory statements," which has been held insufficient by the Supreme Court. *Iqbal*, 556 U.S. at 678.

It would be easy to assert that allegedly shoddy data security has no benefits, but this misses the point: This prong of unfairness requires the FTC to weigh the benefits of the legal burdens it would impose with their costs. However great the benefits of data security, they are not absolute—and still subject to tradeoffs.[11] The

[11] *Unfairness Statement*, 104 F.T.C. at 1073-74 ("Most business practices entail a mixture of economic and other costs and benefits... The Commission is aware of these tradeoffs and will not find that a practice unfairly injures consumers unless it is injurious in its net effects... These include not only the costs to the parties directly before the agency, but also the burdens on society in general in the form of increased paperwork, increased regulatory burdens on the flow of information, reduced incentives to innovation and capital formation, and similar matters.").

FTC ultimately bears the burden of establishing not only a substantial injury, but also that possible benefits to consumers from the practice at issue do not outweigh that injury.[12] To survive a motion to dismiss, the FTC need not perform this cost-benefit analysis, but it must at least allege enough facts on both sides of the equation that the court can draw the reasonable inference that the costs of "reasonable" data security outweigh the benefits of protecting consumers from harms they themselves could not reasonably avoid. *Iqbal*, 556 U.S. at 678.

Here, the costs are not merely the financial expense of improving security in Wyndham's hotels but also changing the basic franchisor/franchisee model by which Wyndham and countless other companies operate by making the franchisor responsible for its franchisees' data security. *See* Brief of Amicus International Franchise Association at 2. Ultimately, these costs are borne by consumers themselves, not companies. Consumers may also bear additional non-financial costs such as increased difficulty of using Internet services (*e.g.*, for reservations) and other electronic payment systems. The Complaint is silent on these many factors, and says almost nothing about the few factors it does identify.

[12] "[U]nfairness requires in essence a full benefit/cost analysis of the practices the Commission seeks to challenge." Beales, *supra* note 2, at n.53.

B. DECEPTION CLAIMS SHOULD BE HELD TO THE HEIGHTENED PARTICULARITY STANDARD OF 9(B).

In order to prove deception, the FTC must prove there is: (1) a representation, omission, or practice (2) that is likely to mislead consumers acting reasonably under the circumstances, and (3) the representation, omission, or practice is material. *Deception Statement*, 103 F.T.C. at 174-75.

Under FRCP 9(b), "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." In other words, such claims must be accompanied by the "who, what, when, where, and how" of the conduct charged. *Vess v. Ciba–Geigy Corp., USA*, 317 F.3d 1097, 1106 (9th Cir. 2003). Rule 9(b) gives defendants "notice of the claims against them, provide[ ] an increased measure of protection for their reputations, and reduce[ ] the number of frivolous suits brought solely to extract settlements." *In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1418 (3d Cir. 1997).

Where a claim sounds in fraud the heightened pleading requirements of 9(b) apply. *In re Suprema Specialties, Inc. Securities Litigation*, 438 F.3d 256, 270 (3rd Cir. 2004). This court should join the growing number of district courts which have concluded that 9(b) applies to FTC deception allegations. *See, e.g., FTC v. Lights of Am., Inc.*, 760 F. Supp. 2d 848 (C.D. Cal. 2010); *FTC v. Ivy Capital, Inc.*, 2011 WL 2118626 (D. Nev. May 25, 2011).

CONCLUSION

For the foregoing reasons, the Wyndham Defendants' Motions to Dismiss should be granted.

Respectfully submitted,

/s/Stephen M. Orlofsky
Stephen M. Orlofsky, Esquire
New Jersey Resident Partner
Rachel J. Gallagher, Esquire
BLANK ROME LLP
301 Carnegie Center, 3rd Floor
Princeton, NJ 08540
Telephone: (609) 750-7700
Fax: (609) 750-7701
Orlofsky@BlankRome.com
RGallagher@BlankRome.com

Attorneys for Amici Curiae TechFreedom, International Center for Law and Economics & Consumer Protection Scholars Justin ("Gus") Hurwitz, Esquire, Todd J. Zywicki, Esquire, and Paul H. Rubin, Ph.D

Of Counsel & On the Brief:

Berin Szoka, Esquire
TechFreedom
Counsel for TechFreedom

Geoffrey A. Manne, Esquire
International Center for Law and Economics
Counsel for the International Center for Law and Economics

Dated: May 3, 2013