Jonathan G. Cedarbaum*
Heather M. Zachary*
Rachel L. Weiner
Daniel Aguilar*
**Pro Hac Vice* Motions Pending
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
Telephone: (202) 663-6000
jonathan.cedarbaum@wilmerhale.com
heather.zachary@wilmerhale.com
rachel.weiner@wilmerhale.com
daniel.aguilar@wilmerhale.com

Attorneys for amicus curiae the International Franchise Association

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

Federal Trade Commission, **Plaintiff,** **v.** **Wyndham Worldwide Corp., et al.,** **Defendants.**	**Civil Action No. 13-cv-1887 (ES) (SCM)** **BRIEF AMICUS CURIAE OF THE INTERNATIONAL FRANCHISE ASSOCIATION IN SUPPORT OF DEFENDANT WYNDHAM HOTELS & RESORTS' MOTION TO DISMISS**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER

INTRODUCTION

The International Franchise Association ("IFA") respectfully submits this brief amicus curiae in support of the motion to dismiss of Defendant Wyndham Hotels & Resorts, LLC ("WHR") in order to apprise the Court of the views of the IFA's 13,000 members regarding two aspects of this novel and important case. First, the Federal Trade Commission's claim that WHR engaged in "deceptive" acts and practices is inconsistent with basic legal principles governing the franchise relationship. Second, the FTC lacks authority to impose data-security requirements on private businesses under the prohibition against "unfair … acts or practices" in Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a)(1).

STATEMENT OF INTEREST

The IFA is the oldest and largest franchise trade association in the world. Founded in 1960, the IFA has more than 1,100 franchisor members that collectively represent a "who's who" of American business: McDonald's, Pizza Hut, Holiday Inn, Hilton, Century 21, and H&R Block, among many others. Since its expansion to include franchisees in 1993, the IFA also represents the interests of approximately 12,000 franchisee members.

The IFA's overall mission is to enhance and safeguard the environment for both franchisors and franchisees, and the franchise business model generally. It

has appeared as amicus curiae to represent the interests of franchise businesses in several federal courts, including the Supreme Court of the United States. The IFA submits this brief to represent the interests of franchise businesses in this litigation.

ARGUMENT

I. THE FTC'S DECEPTION CLAIM IS INCONSISTENT WITH BASIC PRINCIPLES OF FRANCHISE LAW

In Count I of its Amended Complaint, the FTC claims that WHR deceived consumers. Although the FTC alleges "numerous instances" of deceptive practices, Dkt. No. 28, Am. Compl. ¶ 44, in fact the only purported deception identified in the Amended Complaint is WHR's alleged failure to implement data-security measures consistent with its publicly available privacy policy, *id.* ¶¶ 21, 24, which in turn allegedly enabled cyber-criminals to exploit security vulnerabilities through WHR franchisees' computer systems on three occasions, *id.* ¶¶ 26-27, 30, 34-36, 37.

The FTC's claim fails as a matter of law for at least two reasons. First, it ignores the basic legal principle that a franchisor may be held liable for the actions of its franchisee only when it directly controls the franchisee's conduct. *See, e.g.*, *Drexel v. Union Prescription Centers, Inc.*, 582 F.2d 781, 785 (3d Cir. 1978); *see generally* W. Michael Garner, 2 *Franchise and Distribution Law and Practice* § 9:42 (2012) (to determine liability, "the court will look to the franchise agreement for indicia of the franchisor's control over the franchisee" or to any

"actual control exercised by the franchisor over the franchisee"). Far from establishing control, the FTC's allegations reflect WHR's apparent *lack* of control over its franchisees' data-security practices. *See* Am. Compl. ¶ 24. Holding WHR liable in the absence of control would stand basic principles of franchise liability on their head.

Second, the FTC's deception claim overlooks the explicit disclaimer in WHR's privacy policy explaining that franchisees are not covered:

> **Our Franchisees.**
> *Each Brand hotel* is owned and operated by an independent Franchisee that *is neither owned nor controlled by us or our affiliates. Each Franchisee collects Customer Information and uses the Information for its own purposes. We do not control the use of this Information or access to the Information by the Franchisee and its associates.* The Franchisee is the merchant who collects and processes credit card information and receives payment for the hotel services. The Franchisee is subject to the merchant rules of the credit card processors it selects, which establish its card security rules and procedures.

Dkt. No. 91-3, Hradil Decl., Ex. A (emphases added). On its face, the privacy policy makes data-security representations only with respect to WHR—whereas the alleged data-security breaches at issue here apparently originated through attacks by Russian hackers on franchisees' systems.

The express disclaimer of responsibility in WHR's privacy policy is consistent with basic principles of franchise law. A franchise is a contractual relationship in which the franchisor—the owner of a business concept and the

associated trademarks or service marks—authorizes a franchisee to conduct a business that is identified by the franchisor's marks and uses the franchisor's operational format. *See generally* Black's Law Dictionary 729 (9th ed. 2009). The contractual relationship is defined by a franchise or license agreement, which sets forth the obligations of franchisor and franchisee. *Id.*

The franchise business model is an enormously successful form of economic enterprise, as evidenced by its widespread adoption by some of the Nation's most successful companies. As of 2007 (the most recent year for which data is available), more than 800,000 franchise-business establishments directly employed more than nine million people and contributed $468.5 billion to the gross domestic product.[1]

This widespread success is due to the franchise business model itself, which allows the franchisee to operate as an independent business enterprise. Franchising relies upon the franchisee's entrepreneurial spirit and profit incentive to expand the company brand and produce a quality product. "The franchisor utilizes the system to distribute his products or capitalize upon his service marketing scheme without the need of establishing his own related marketing divisions and thus utilizes the network to do his business or an essential aspect of it for him. The franchisee

[1] IFA, III *The Economic Impact of Franchised Businesses* I-14 (2011), http://www.buildingopportunity.com/download/National%20Views.pdf.

receives the benefit of the franchisor's know-how and reputation and contributes his own capital and labor." *Neptune T.V. & Appliance Serv., Inc. v. Litton Microwave Cooking Prods. Div., Litton Sys., Inc.*, 462 A.2d 595, 600 (N.J. Super. Ct. App. Div. 1983). The franchise relationship, while mutually beneficial, is less like a partnership agreement, see *id.* (citing *Lobdell v. Sugar 'N Spice, Inc.*, 658 P.2d 1267, 1273-1275 (Wash. Ct. App. 1983)), and is more "akin to that of a limited independent contractor" agreement, without "absolute control [by one party] over the other," *Lobdell*, 658 P.2d at 1274.

Franchisees—who are often "experienced and sophisticated businessmen"—deliberately negotiate with franchisors to reach a mutually agreeable business arrangement. *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 484-485 (1985) (describing arm's length bargaining between franchisors and franchisees). In the franchise agreement, the parties will often agree that the franchisee is acting as an independent contractor, which allows the parties to retain clearly separate legal statuses and allows each party to employ its own agents. *See, e.g., Simpkins v. 7-Eleven, Inc.*, 2008 WL 918482, at *4 (N.J. Super. Ct. App. Div. Apr. 7, 2008) (citing franchise agreement to show that franchisee was an "independent contractor" with "control [over] the manner and means of operation," including employment decisions); *Chen v. Domino's Pizza, Inc.*, 2009 WL 3379946, at *3

(D.N.J. Oct. 16, 2009) (franchisor has no direct relationship with franchisee's employees).

Consistent with the franchisee's status as a separate and independent actor, a franchisor may ordinarily be held liable for the actions (or inactions) of its franchisee only when the franchisor has the "right to control" the franchisee with respect to the matter at issue. *See Drexel*, 582 F.2d at 785 ("the basic inquiry is whether" the franchisee "is subject to the alleged [franchisor's] control or right to control with respect to … the performance of the services for which [it] was engaged" (internal quotation marks omitted)); Martin D. Fern, *Establishing and Operating under a Franchise Relationship* § 1.04[3][C] (2000) ("A franchisor, however, is generally not vicariously liable for the acts or omissions of its franchisees."). In applying the right-to-control test, courts typically look both to the rights granted in the franchise agreement and to the actual control exerted by the franchisor. "[T]he right to conduct periodic inspections to ensure consistency and quality of the [] brand does not give rise to the power to control the daily maintenance of the premises." *Capriglione v. Radisson Hotels Int'l, Inc.*, 2011 WL 4736310, at *3 (D.N.J. Oct. 5, 2011); Garner § 9:42 ("Apart from the agreement, courts look to the actual control exercised by the franchisor over the franchisee."). To be liable for a franchisee's actions and responsibilities, the franchisors must "exercise more [control] than a right to control uniformity of

appearance, products and administration." *Capriglione*, 2011 WL 4736310, at *3; *see also Fry v. Industrial Comm'n of Ariz.*, 546 P.2d 1149, 1151-1152 (Ariz. Ct. App. 1976) (holding that 7-Eleven franchisee, engaged in normal franchise relationship, was an independent contractor of franchisor); *Karnauskas v. Columbia Sussex Corp.*, 2012 WL 234377, at *3 (S.D.N.Y. Jan. 24, 2012) (franchisor may be held liable only if "the [franchisor] has considerable day-to-day control over the specific instrumentality that is alleged to have caused the harm").[2]

Hence, if a franchise is "individually owned and operated as an individual business," as is typically the case, then the franchisor's mere status as franchisor "does not evince the degree of control that would warrant the imposition of vicarious liability under agency principles." *J.M.L. ex rel. T.G. v. A.M.P.*, 877 A.2d 291, 297 (N.J. Super. Ct. App. Div. 2005); *see also Dubois v. Kepchar*, 889 F. Supp. 1095, 1102-1103 (N.D. Ind. 1995) (rejecting the argument that just "because McDonald's requires franchisees to erect golden arches out front, it should be held liable if a customer is sickened by improperly cooked meat"). "[T]he mere fact that a franchisor's sign appears on a building and the employees within that building wear uniforms bearing the franchisor's logo and insignia does

[2] In *Capriglione*, the Court noted the inability of the plaintiffs or the Court to find "a single case that supports the proposition that a franchisor has a duty to the guest of a hotel of which it does not directly own or exercise control." *Capriglione*, 2011 WL 4736310, at *3.

not clothe a franchisee with the apparent power to act on the franchisor's behalf in anything approaching a general way." *Pona v. Cecil Whittaker's, Inc.*, 155 F.3d 1034, 1036 (8th Cir. 1998) (rejecting ADA complaint brought against franchisor for franchisee's alleged discrimination).

Similarly, employees of a franchisee are not considered to be employed by the franchisor unless the franchisor had "control over its franchisee's labor relations or financial control over the franchisee," even if the franchisor "may have stringently controlled the manner of its franchisee's operations, conducted frequent inspections, and provided training for franchise employees." *Lockard v. Pizza Hut, Inc.*, 162 F.3d 1062, 1070 (10th Cir. 1998) (internal quotation marks omitted). Likewise, a hotel franchisor will not be liable for a guest's injury or loss of property at a franchisee hotel if the franchisee manages the "day-to-day" operation of the hotel. *Schwartz v. Hilton Hotels Corp.*, 639 F. Supp. 2d 467, 469, 472-473 (D.N.J. 2009); *Schear v. Motel Mgmt. Corp. of Am.*, 487 A.2d 1240, 1249 (Md. Ct. Spec. App. 1985).

Under these black-letter principles governing franchisor-franchisee relations across the realms of contract, tort, employment, and property law, a franchisor may not be held liable for its franchisee's data-security failings when the franchisor does not control the day-to-day security of the franchisee's computer systems. Permitting franchisors to be held liable for data breaches that occur through their

franchisees' computer systems regardless of their right to control their franchisees' data-security measures may discourage franchisors from expanding their franchises beyond what they can directly monitor and control. Franchisors could be forced to divert resources to observing and regulating their franchisees' computer-network security in order to limit their potential liability. They might terminate some franchise agreements to save on this monitoring cost. And entrepreneurs wishing to become franchisees could face higher barriers to entry due to these increased costs.

Here, the FTC does not allege that WHR had a legal right to control its franchisees' data-security practices. Although the FTC conclusorily alleges that WHR actually controls the customer data collected by its franchisee hotels, *see* Am. Compl. ¶¶ 15-17, the FTC fails to include any plausible factual basis for this averment. "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "Where a complaint pleads facts that are 'merely consistent' with a defendant's liability, it 'stops short of the line between possibility and plausibility of "entitlement to relief."'" *Id.* at 667 (quoting *Twombly*, 550 U.S. at 557). The FTC does not plausibly allege that WHR actually controls its franchisees' data entry or local data security. To the contrary, the FTC

claims that one of the reasons WHR acted unreasonably is that it *failed* to do so. *See* Am. Compl. ¶ 24. These allegations hardly suffice to show that WHR actually controlled (or had a right to control) its franchisees' data-security practices. And if sustained, the FTC's theory would turn franchise law on its head by affirmatively *requiring* franchisors to assume control over data security across their franchise locations. Therefore, WHR should not be held liable for any data breach that allegedly occurred because of its franchisees' purported data-security vulnerabilities.

In any event, there is no basis for holding a franchisor like WHR liable for deception where its privacy policy expressly disclaimed any responsibility for the data-security practices of its franchisees. The privacy policy that forms the basis for the FTC's allegation that WHR engaged in deceptive practices expressly states that "[e]ach Brand hotel is owned and operated by an independent Franchisee that is neither owned nor controlled by [WHR] or [its] affiliates. Each Franchisee collects Customer Information and uses the Information for its own purposes. [WHR] do[es] not control the use of this Information or access to the Information by the Franchisee and its associates." Dkt. No. 91-3, Hradil Decl., Ex. A. Whatever promises WHR's privacy policy allegedly makes to consumers, these representations plainly do not extend to the data-security practices of WHR's franchisees.

II. THE FTC DOES NOT HAVE AUTHORITY TO REGULATE DATA SECURITY UNDER SECTION 5'S PROHIBITION ON UNFAIR ACTS OR PRACTICES

As an alternative ground for liability, the FTC claims in Count II of its Amended Complaint that WHR engaged in an "unfair" act or practice. This claim rests on the allegation that WHR, as a franchisor, "failed to employ reasonable and appropriate measures to protect personal information against unauthorized access." Am. Compl. ¶ 47. The IFA agrees fully with WHR that this claim fails as a matter of law because the FTC lacks authority, under the guise of its general power to police "unfair … acts or practices," 15 U.S.C. § 45(a)(1), to impose a data-security code on American businesses.

The FTC Act, originally enacted in 1914, prohibits "unfair … acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). An act or practice may be deemed "unfair" only if it 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." *Id.* § 45(n). The FTC is authorized to prevent "unfair" acts or practices, *id.* § 45(a)(2), and to bring a civil action to enjoin those acts or practices, *id.* § 53(b). Although this power to prevent unfair business practices is arguably broad, *see American Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 967-968 (D.C. Cir. 1985), it is certainly not unlimited. The

FTC's novel interpretation of Section 5's unfairness prohibition should be rejected for at least two fundamental reasons.

First, where Congress has authorized a federal agency to impose data-security requirements on the private sector—as it has done repeatedly with respect to particular industries—it has done so expressly, rather than implicitly through general and indirect provisions such as Section 5. It is well established that the "meaning of one statute may be affected by other Acts, particularly where Congress has spoken subsequently and more specifically to the topic at hand." *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000). That is just what has happened with respect to data-security regulation.

Although the FTC Act may authorize the FTC "to take action against unfair practices *that have not yet been contemplated by more specific laws*," *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1194 (10th Cir. 2009) (emphasis added), over the past 20 years Congress has enacted many statutes that expressly authorize particular agencies to establish mandatory privacy and data-security standards for private firms (such as health-care providers and financial institutions) that handle particular types of data (such as personal health information and personal financial information).[3] Indeed, in a number of these statutes (none of which is applicable

[3] *See, e.g.*, Fair and Accurate Credit Transactions Act of 2003, Pub L. No. 108-159, §§ 411-412, 117 Stat. 1952, 1999-2003, 15 U.S.C. §§ 1681 *et seq.*;

here)—such as the Fair and Accurate Credit Transactions Act of 2003, the Children's Online Privacy Protection Act, and the Gramm-Leach-Bliley Financial Services Modernization Act—Congress explicitly authorized the FTC to enforce certain specific data-security requirements for limited categories of data in particular industries. Where, as here, an "earlier statute is broad but the subsequent statutes more specifically address the topic at hand," the subsequently enacted specific statutes "shape or focus" the meaning of the previously enacted statute, thus limiting its application "even though it ha[s] not been expressly amended." *Brown & Williamson Tobacco*, 529 U.S. at 143 (internal quotation marks omitted); *United States v. Fausto*, 484 U.S. 439, 452-453 (1988) (similar). These specific and recently enacted statutes, rather than the general and vague "fairness" dictate of the FTC Act, establish the precise data-security obligations of American businesses and define the outer boundaries of the FTC's authority to regulate the

---

Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501-503, 113 Stat. 1338, 1436-1440 (1999), 15 U.S.C. §§ 6801 *et seq.*; Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, §§ 1301-1303, 112 Stat. 2681-728 to 2681-732, 15 U.S.C. §§ 6501 *et seq.*; Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, § 262, 110 Stat. 1936, 2021-2029 (1996), 45 U.S.C. §§ 1320d *et seq.*; Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, §§ 13101-13424, 123 Stat. 115, 228-279 (2009), 42 U.S.C. §§ 17921 *et seq.*; Cable Television Consumer Protection and Competition Act of 1992, Pub. L. No., 102-385, § 20, 106 Stat. 1460, 1497-1498, 42 U.S.C. §§ 551 *et seq.*

private sector's data-security practices.[4]

Second, the statutory prohibition against "unfair" business practices is precisely the kind of open-ended provision that should not be understood to empower an administrative agency to impose sweeping changes in the practices of American businesses, such as the data-security obligations the FTC seeks to impose here. *Cf., e.g.*, *Gonzales v. Oregon*, 546 U.S. 243, 267 (2006) (Attorney General lacks authority under controlled-substances laws to prohibit doctors from prescribing drugs for use in physician-assisted suicide); *Brown & Williamson Tobacco*, 529 U.S. at 133, 160-161 (FDA lacks authority to regulate marketing of tobacco products as "drugs" or "devices"); *MCI Telecomms. Corp. v. AT&T Co.*, 512 U.S. 218, 231 (1994) (FCC may not make tariff filing entirely optional under its authority to "modify" requirement to file tariff). Indeed, for nearly two years, Congress has been embroiled in an historic debate over almost a dozen data-security bills that seek to strike a proper balance between, on the one hand, requiring detailed data-security measures to defend against an array of cyber threats to our national and economic security and, on the other hand, avoiding excessive and intrusive regulation that could damage the nation's fragile economic

[4] The President, in signing Executive Order 13636, 78 Fed. Reg. 11739 (Feb. 12, 2013), chose to entrust the National Institute of Standards and Technology—not the FTC—with developing a voluntary program to establish a data-security framework. *Id.* § 7.

recovery. If the FTC's position were correct, this fundamental debate in Congress would have been unnecessary.

CONCLUSION

For the foregoing reasons, amicus curiae the International Franchise Association respectfully submits that the Court should grant Defendant WHR's motion to dismiss.

Dated: May 3, 2013

Respectfully submitted.

/s/ Rachel L. Weiner
Jonathan G. Cedarbaum*
Heather M. Zachary*
Rachel L. Weiner
Daniel Aguilar*
**Pro Hac Vice* Motions Pending
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
Telephone: (202) 663-6000
jonathan.cedarbaum@wilmerhale.com
heather.zachary@wilmerhale.com
rachel.weiner@wilmerhale.com
daniel.aguilar@wilmerhale.com