FTC’s Data Security Authority Survives Challenge in Wyndham

By Matthew B. Gruenberg, David W. Nelson

A recent ruling in the Federal Trade Commission’s closely watched data security lawsuit against Wyndham Worldwide Corporation (Wyndham) could bolster the FTC’s efforts to regulate data security. Denying a motion to dismiss in Federal Trade Commission v. Wyndham Worldwide Corporation, Case No. 13-cv-01887, the U.S. District Court for the District of New Jersey upheld an FTC civil complaint against Wyndham and its subsidiaries arising from data-security breaches on computer systems operated by Wyndham and its franchisees.

The court’s decision affirms the FTC’s authority over data security under Section 5 of the Federal Trade Commission Act. This ruling should be a wake-up call for all businesses that handle consumer data, but it has particularly important implications for franchisors, who now must evaluate their obligations to ensure proper data-security practices on franchisee-controlled computer systems that connect to a franchisor-controlled or shared network.

Acts Deemed “Unfair,” “Deceptive”

Through its subsidiaries, Wyndham has franchise agreements with approximately 75 independently owned hotels and management agreements with approximately 15 independently owned hotels. The agreements require these “Wyndham-branded hotels” to purchase designated computer systems and configure them to Wyndham’s specification. These “property management systems” are used by each hotel to handle reservations, check guests in and out, assign rooms, manage room inventory, and handle payment card transactions. They store consumer information, including...
names, contact information, and credit card information, on the Wyndham-branded hotels’ servers.

Each Wyndham-branded hotel’s system is then linked to Wyndham’s corporate network, including its central reservation system. The property management systems are owned by each individual Wyndham-branded hotel, run off of each hotel’s own servers, and operated by each hotel’s own employees. Nevertheless, the FTC alleges that Wyndham “managed” the systems because it had exclusive administrative access and set all rules for the systems, including password requirements that allowed the Wyndham-branded hotels’ employees to access the systems.

On three separate occasions between April 2008 and January 2010, cyber-attackers gained unauthorized access to Wyndham’s corporate network and to many of the Wyndham-branded hotels’ property management systems. Through that access, the attackers obtained consumer information stored on the Wyndham-branded hotels’ property management systems. The FTC alleges that more than 619,000 consumer payment card account numbers were compromised in these data breaches, resulting in more than $10.6 million in fraud.

The FTC attributed these data breaches to Wyndham’s failure to provide reasonable security for the consumer information maintained both in its corporate network and on the Wyndham-branded hotels’ property management systems. The FTC alleges that these failures were “unfair,” and that Wyndham’s representations on its website that it had implemented reasonable and appropriate security measures were “deceptive” under Section 5(a) the FTC Act.

Court Upholds FTC’s Authority under Section 5(a) of FTC Act

With the support of several trade organizations, including the International Franchise Association and the Chamber of Commerce of the United States, Wyndham brought a motion to dismiss, challenging, in part, the FTC’s authority to regulate a private company’s data security practices as “unfair acts or practices” under Section 5(a) of the FTC Act. Section 5(a) defines an “unfair act or practice” to include one that “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and [is] not outweighed by countervailing benefits to consumers or to competition.” 15 U.S.C. § 45(n).

Relying primarily on FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120 (2000), in which the United States Supreme Court found that the Food and Drug Administration (FDA) did not have authority to regulate tobacco products because Congress intended
to exclude them from the FDA’s jurisdiction, Wyndham argued that recent data-security law—including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the Children’s Online Privacy Protection Act, and the Health Insurance Portability and Accountability Act—show Congress’s intent to authorize “particular federal agencies to establish minimum data-security standards in narrow sectors of the economy.” Allowing the FTC to establish general data-security standards for the private sector under Section 5 of the FTC Act would be incompatible with this “overall statutory landscape,” Wyndham argued.

The court rejected this argument, refusing to “carve out a data-security exception to the FTC’s unfairness authority.” In this case, unlike in the Brown decision on the FDA’s authority, the court refused to find that the FTC’s authority over data security was “incompatible with more recent legislation” or that it “plainly contradict[ed] congressional policy.” Instead, the court concluded that recent legislation dealing with data security complements, and does not preclude, the FTC’s authority.

The court also found that Wyndham had received fair notice that “unreasonable data security practices” were “unfair” under Section 5 of the FTC Act, rejecting Wyndham’s argument that fair notice required the FTC to publish formal rules and regulations before bringing an enforcement action. The court explained that the contour of an unfairness claim in the data-security context must be “flexible,” so that “the FTC can apply Section 5 to the facts of particular cases arising out of unprecedented situations.” Thus, the court concluded, the FTC Act’s test under 15 U.S.C. § 45(n) to determine whether an act is “unfair” (stated above) and the FTC’s many public complaints and consent agreements, as well as its public statement and business guidance brochure, provided adequate notice of the data-security standards under Section 5.

Finally, the court rejected Wyndham’s contention that the FTC failed to allege substantial, unavoidable consumer injury sufficient to show that Wyndham’s practices were “unfair” under 15 U.S.C. § 45(n). The court concluded that the FTC’s allegation of small losses to many consumers constituted “substantial injury to consumers.” More notably, the court concluded that the FTC had pled that Wyndham “caused” substantial injury to consumers through allegations that Wyndham’s unreasonable data-security practices allowed the cyber-attacks to occur, which ultimately resulted in consumer injury.

**Privacy Policy Claim Survives**

The district court also denied Wyndham’s effort to dismiss the FTC’s “deceptive” practices claim. The FTC alleged that statements on Wyndham’s website and in its privacy policy that it had “implemented reasonable and appropriate measures to protect personal information against unauthorized access” were false or
misleading and constitute deceptive practices under Section 5(a) of the FTC Act. Wyndham argued that these statements were not deceptive because they were expressly limited to information maintained on Wyndham-controlled computer systems. By contrast, the consumer information taken in the cyber-attacks was stored on the Wyndham-branded hotels’ property management systems.

In rejecting this argument, the court concluded it could not make a determination at the pleading stage that Wyndham and the Wyndham-branded hotels are, as a matter of law, separate entities with their own computer networks and data-collection practices. Moreover, the court found that a reasonable consumer would not have understood Wyndham’s statements to include only data-security practices on Wyndham’s corporate system and not on the Wyndham-branded hotels’ systems.

**Implications for Franchisors**

Even though Wyndham has filed an interlocutory appeal to the Third Circuit, and even though this is merely a district court order on a motion to dismiss, the Wyndham decision will likely add momentum to the FTC’s recent efforts to regulate data-security practices through enforcement actions over data-security breaches (most of which are now resolved through potentially costly consent decrees).

Yet the decision provides little guidance for businesses regarding what constitutes “reasonable” data-security measures. The court acknowledged that this is a fact-specific inquiry that will vary from business to business. Despite this limited guidance, however, businesses would be wise to reevaluate their data-security practices to identify and address potential risks to their systems.

For franchisors, this may mean ensuring that proper data-security practices are followed by franchisees that connect franchisee-controlled computer systems to the franchisor’s corporate system or to shared systems controlled by the franchisor. The FTC’s allegations against Wyndham are based, in part, on Wyndham’s failure to ensure that the Wyndham-branded hotels implemented proper data-security measures on their property management systems before connecting to Wyndham’s corporate system, as well as on Wyndham’s failure to properly limit access between and among the corporate system, the property management systems, and the internet.

Further, franchisors should consider whether the requirements they establish for their franchisees’ computer systems, or the control they exercise over those systems, may give rise to an obligation to ensure that franchisees are following proper data-security practices, and may give rise to potential liability if there is a data-security breach on the franchisee’s local system.
The authors thank Kristyn Gregor, Barnes & Thornburg, LLP, for her contributions to this article.