

# Privacy Alert – FTC Action May Turn Traditional Concepts of Privacy Enforcement and Franchise Law on Their Heads

December 17, 2013

The franchise community is taking center stage in an ongoing privacy case that, for the first time, challenges the very authority of the Federal Trade Commission (FTC) to regulate the data security practices of private businesses. In the same case, the FTC also seeks to hold a franchisor responsible for data security breaches it claims occurred primarily among its independently owned franchisees, even though the franchisor disclaimed responsibility for its franchisees' data security practices in an online privacy policy. Under the circumstances, this case could have far reaching effects not only in the world of privacy law, but in the franchise community as well.

## **Background**

In June 2012, the FTC filed a complaint against a franchisor, Wyndham Hotels & Resorts, LLC (Wyndham), and independently owned franchisees within its system under Section 5 of the FTC Act, which generally prohibits "unfair or deceptive acts or practices in or affecting commerce." In its two-count complaint, the FTC alleges that Wyndham and its franchisees engaged in: (1) "deceptive" practices by misrepresenting in sales and marketing materials that they used "industry standard practices" and "commercially reasonable efforts" to secure the data they collected from their guests; and (2) "unfair" practices because their lax security measures failed to protect this data.

It is generally undisputed that from 2008 to 2010, a criminal organization based in Russia used sophisticated malware to hack into computer servers maintained by Wyndham and/or its franchisees, ultimately accessing credit card information from several hundred thousand guests of Wyndham-branded hotels, resulting in \$10.6 million in fraud losses.

For its remedies, the FTC seeks both monetary damages and a permanent injunction requiring Wyndham and its franchisees to better secure their systems. Wyndham filed a motion to dismiss the FTC action, and a hearing on that motion was held in the New Jersey District Court on November 7, 2013.

**Privacy Law Issue: Does the FTC have the authority to regulate and impose data security standards on private businesses under the FTC Act?**



The FTC has been increasingly aggressive in bringing enforcement actions against private businesses under the FTC Act following data privacy and security breaches. Because these actions generally have been resolved through settlements and consent decrees, there are very few court opinions defining the boundaries of FTC authority in this area.

In fact, Wyndham is the first company to overtly challenge the FTC's authority to regulate and impose data security standards on businesses through enforcement actions under the FTC Act. In its motion to dismiss, Wyndham essentially argues that Congress never granted the FTC such broad authority to regulate in this area, and, even if it did, the FTC has not provided businesses with fair notice of what data security practices it believes the FTC Act forbids or requires.<sup>1</sup>

**Franchise Law Issue: Are franchisors legally responsible for the data privacy and security practices of their franchisees?**

While privacy professionals are focusing on the Wyndham case because of Wyndham's challenge to the FTC's authority in this area, the franchise community is equally concerned about whether, and under what circumstances, franchisors may be responsible for data security breaches attributed to independently owned franchisees within their systems. As in other contexts, the answer to this question will turn on the facts and circumstances of the case, and particularly the level of control the franchisor is found to have exercised over the data collected by its franchisees, as well as the security measures they used to protect that data.

In an effort to pin liability for the data security breaches at issue on Wyndham, the FTC alleges that Wyndham exercised actual control over the data its franchisees collected and the relevant aspects of the systems they used to secure the data. For example, the FTC alleges that Wyndham managed its franchisees' data security systems, administered access to those systems, set passwords for the systems, and provided exclusive technical support for the systems. The FTC also alleges that before franchisees were allowed to connect their local computer networks to Wyndham's corporate network—thereby creating a single, coordinated network that ultimately failed, at least according to the FTC—Wyndham did not ensure its franchisees implemented adequate data security policies and procedures. For these and other reasons, the FTC argues that Wyndham cannot disclaim responsibility for the data security failures it attributes to its franchisees.

In response to these allegations, Wyndham argues that as with most franchise systems, Wyndham and its independently owned franchisees are separate and distinct legal entities that maintain separate computer networks and engage in their own data collection practices. Wyndham also argues that statements it makes in its online privacy policy—which provide the sole basis for the FTC's deception claim—relate only to the privacy policies and practices of Wyndham (the franchisor), and not to those of its franchisees. Finally, Wyndham emphasizes that within its privacy policy, it **expressly disclaims** responsibility for the security of customer data collected by its franchisees:



## **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.

On behalf of Wyndham and the franchise community at large, the International Franchise Association (IFA) weighed in with an amicus brief in the Wyndham case. In essence, the IFA argues that if the court sustains the FTC's theory of franchisor liability under these circumstances, it "would turn franchise law on its head by affirmatively requiring franchisors to assume control over data security across their franchise locations." And if that happens, the IFA further argues that franchisors would be: (1) discouraged from expanding their systems beyond what they can directly monitor and control; (2) forced to divert resources to observing and regulating their franchisees' computer networks; and (3) forced to terminate franchise agreements in order to save on monitoring costs.

## **Conclusion**

It is unclear when we might have a final resolution of the Wyndham case, but a ruling on Wyndham's motion to dismiss could come any day. Given the importance of the issues raised in Wyndham for the franchise community at large, we will continue to provide updates on this case and other privacy cases of interest to the franchise community.

If you have any questions on this client alert please contact Brian Dillon or Michael Cohen.

---

<sup>1</sup> It should be noted that LabMD, a medical testing provider, recently followed Wyndham's lead and filed a motion to dismiss a different FTC enforcement action on the same grounds.

*This article is provided for general informational purposes only and should not be construed as legal advice or legal opinion on any specific facts or circumstances. You are urged to consult a lawyer concerning any specific legal questions you may have.*