Protecting Your System From Cybersecurity Attacks

While the news headlines in 2015 trumpeted the latest data breaches from Anthem to United Airlines, courts and federal agencies have grappled with how to define a company's legal obligation to stay one step ahead of criminal hackers in protecting consumers' private information. The most important recent legal development in the context of a franchise system is the Third Circuit Court of Appeals' decision in *Federal Trade Commission v. Wyndham Worldwide Corp.*, which was decided on August 24, 2015. While the decision involved procedural issues (the issue of the franchisor's liability for a security breach is pending), it's a clear reminder to every franchisor to evaluate how it and its franchisees collect and protect consumer data. Is your brand at risk?

Like many franchise systems, Wyndham maintained a database containing customer information including names, addresses, credit card numbers, and expiration dates. Each hotel collected the data from its consumers, and the franchisor collected and maintained the data in a central database. The data was hacked on three separate occasions – one involving the franchisee's local system, and the other two involving the franchisor's central database – resulting in the alleged theft of private data from more than 600,000 Wyndham customers and more than $10 million in fraudulent credit card charges.

The FTC filed a lawsuit against the franchisor and its related entities alleging that they engaged in inadequate cybersecurity practices that unreasonably exposed customers' data to hackers. The FTC detailed that Wyndham failed to encrypt credit card information, permitted easily-guessed passwords, and did not employ firewalls, among others, which allowed hackers to access the local network and then infiltrate an administrative account by guessing the passwords. The FTC claimed that Wyndham did not take reasonable counter-measures to detect security breaches or to follow appropriate response procedures. Indeed, the FTC noted that Wyndham itself did not learn of the attacks until eight months after the first incident.

The issue before the appellate court was not whether Wyndham was liable for the breach – that issue is pending before the trial court - but rather whether the FTC could bring a suit at all against a franchisor that failed to protect its data. The court found that it could and held that the FTC's congressional authority to regulate unfair methods of competition extends to cases where a company presents a privacy policy to entice customers into entrusting it with their private information, and then fails to "make good on that promise by investing inadequate resources in cybersecurity" and thereby exposes them to financial injury. As a result, the case against Wyndham will proceed in the federal trial court.

The court pointed to an FTC-published checklist of practices that form what the FTC calls a "sound data security plan." The court emphasized that this checklist recommends, for instance, encrypting sensitive information, installing firewalls, monitoring the network for breaches, password management, and setting access controls to limit access to only those who have a legitimate business need to use the information. The criticism, of course, is that the FTC's guidelines provide no safe harbor and its advice lacks specificity. The court observed, however, that Wyndham, in this case, allegedly did not employ these measures at all.

The *Wyndham* case provides a basis to ask your management these key questions: What are our cybersecurity defenses and are they up to date? Are we training personnel and franchise owners on data privacy? What are we doing to monitor the network, and what is our plan if the network is breached? For good measure, the court in the *Wyndham* case also noted a disconnect between Wyndham's privacy policy (as stated on its website) and the security measures that it, in fact, implemented. This comment highlights the importance to franchisors of periodically reviewing the online descriptions of their privacy policies to make sure they're delivering the promised protections.

This decision was rendered with regard to specific facts – the system that was hacked was under the franchisor's, not a third-party's, control; the franchisees had access to the central system on which consumer data collected from all sources was stored; and both the franchisor and franchisee were hacked. Your data collection and storage process might be different, so your risk profiles might also be different, and those differences should guide your actions around issues like whether to implement and enforce a system-

wide data privacy policy, for example, and the potential for exposure to vicarious liability as a result of those efforts.

While it may well be impossible to avoid all risks of hacking and the lawsuits and regulatory investigations that may follow, this case highlights that severe consequences can flow from not making reasonable attempts to do so. Franchisors will want to watch how this case develops and, ultimately, how the trial court views the franchisor's culpability for these hacks. Meanwhile, franchisors should be vigilant, implement reasonable security measures, prepare a response plan, and hope to never have to use it.

For questions or more information regarding this Alert, please contact us.

October, 2015

Contacts	Contact Information
Amy Cheng	312-243-1716 or amy.cheng@chengcohen.com
Fredric A. Cohen	312-243-1717 or fredric.cohen@chengcohen.com
Michael R. Daigle	312-957-8366 or michael.daigle@chengcohen.com