

Cybersecurity: New Front for Attacks on Franchise Model

Much has been written on the growing risks of data breaches and other cyberattacks, especially after the massive security breach at Equifax in September 2017. Recent cases holding franchisors liable for franchisees' data breaches are creating a dilemma for franchisors. Below we provide tips on how to help franchisees protect customer data while not unduly creating liability risk for the franchisor.

Aarons Case: (Michael Peterson, et al v. Aaron's, Inc., et al., U.S. District Court, N.D. Georgia, ¶15,562, (Jun. 4, 2015):

In this case, a franchisor was held liable for breach of consumer privacy by its franchisees. Aaron's and its franchisees rent equipment, including computer equipment. Aaron's franchisees installed computer-monitoring software in computers available for rent to consumers. According to the FTC press release, the software "surreptitiously tracked consumers' locations, captured images through the computers' webcams", captured users' login credentials, all without the knowledge of the consumer. The software allowed the franchisees to disable a computer remotely. According to the complaint, "Aaron's franchisees used this illicitly gathered data to assist in collecting past-due payments and recovering computers after default."

The FTC found that Aaron's—by "enabling their franchisees to use this invasive software"—was itself in violation of the consumer's rights, and had violated the FTC rules against deceptive practices, even though this software was not used in any of the company-owned stores. While Aaron's did not use this technology in its company-owned stores, the FTC determined that Aaron's "knowingly assisted its franchisees" in implementing and using this software. Specifically, Aaron's: (1) allowed its franchisees to access the software designer's website to use the software; (2) used its server to transmit and store content from the monitoring; (3) provided franchisees with software technical support. The FTC Consent Order prohibited Aaron's, among other things, from collecting or using customer data without their consent.

Related Capabilities

- Franchise & Distribution Law

This case illustrates that “bad facts make bad law.” This monitoring software seemed to have clearly violated consumer privacy expectations. The franchisor did more than specify a third party supplier, it participated in support for the software. Therefore the case also stands for the proposition that a franchisor is liable for the acts of a franchisee where the franchisor participates. Of course a franchisor should just say no when it learns of franchisee practices that are clearly illegal or wrong. However, franchisors must be careful to not have too much involvement in a franchisee’s privacy and security policies, to avoid being held liable for franchisee-caused problems. Best practices are summarized at the end of this blog.

Accordingly, franchisors may wish to review their policies related to privacy and security, and their instructions and principles for franchisees, including any ongoing monitoring and auditing. Moreover, a franchisor should use a privacy officer or outside consultant with adequate expertise and training to assess information gathering activities of both the franchisor and the franchisees to reduce the risks of non-compliance with laws and of data breaches.

Wyndham Case: (FTC v. Wyndham Worldwide Corporation, et al., U.S. Dis Ct, D. New Jersey, ¶15,249, 10 F. Supp. 3D602, (Apr. 7, 2014):

Wyndham is another case in which a franchisor was alleged to be liable for technology practices of franchisees, in this case data security breaches. However, unlike Aaron’s the underlying practices were not obviously wrongful.

Wyndham’s franchisee was hacked in Phoenix in 2008, by sophisticated criminal hackers, who obtained hotel level consumer credit card numbers. Wyndham’s systems were accessed, but information was lost only from the franchisee. Wyndham had an incident response plan that involved immediately hiring forensic experts, notifying affected employees, franchisees, customers, credit card companies, and government agencies. The credit card companies offered consumers credits for any fraudulent charges, so no consumer was harmed.

However, April 2010 FTC began to investigate, alleging that the franchisor had unreasonable practices, and alleging that the franchisor was taking responsibility for all 7000 franchisees’ data practices. In July 2010, Wyndham refused to sign the FTC’s proposed consent order, so the FTC filed a lawsuit. The FTC cited Wyndham for nine practices that did not meet the FTC’s standards.

All of the consumer information was stolen at franchisee level. The FTC wanted to hold the franchisor liable for the alleged information security deficiencies of the franchisee. The franchisor’s defense was that it had no duty for franchisee’s security breach.

The third circuit decided against Wyndham on two ancillary matters, but agreed that there needed to be more than inconvenience to consumers. Thereafter Wyndham and the FTC settled in 2015, and signed a Consent Order. The FTC dropped its theory of liability of the franchisor for franchisee data breach in this Consent Order. In the Consent Order Wyndham must maintain certain standards for payment card data security.

Dorsey Dos and Don'ts for Franchisors:

1. *Say no when a franchisor learns of franchisee privacy and data security practices that are clearly illegal or wrong.*
2. *Provide third party training and support to franchisees related to privacy and data security from competent and reputable experts. For example a franchisor can refer franchisees to third party trainers and cybersecurity experts to maintain payment card (PCI) compliance.*
3. *Do not have too much involvement in a franchisee's privacy and security policies, to avoid being held liable for franchisee-caused problems. Only if the franchisor has the expertise (or hires it) should it try to manage a franchisee's data collection and protection.*
4. *Provide franchisees with information on what they must do if there is a data breach, and have in place a franchisor data breach incident response plan as well. Such plans are governed by state and federal law, so consult a privacy lawyer to implement such a plan.*

Dorsey's Privacy and Data Protection lawyers can give specific advice on your specific system issues. The above is general advice that is not tailored to a specific franchise system.

Contact: Gary R. Duvall at (206) 903-8700 or Josh Piper at (206) 903-5428