FRANCHISE & DISTRIBUTION

NAVIGATING THE CYBER LIABILITY STORM – PART I

by Andrae J. Marrocco

Franchisors are facing a precarious three-way intersection of increased accountability and regulation over consumer privacy, the growing volume and sophistication of cyber-attacks on consumer data, and the expanding boundaries of franchisor liability for matters arising at the franchise unit level.

Two recent cases have raised awareness of the risky climate for franchisors in the realm of cybersecurity and privacy compliance.

Aaron's, Inc.[1]

On March 10, 2014, the Federal Trade Commission ("FTC") approved a final order settling charges that the franchisor knowingly assisted its franchisees to engage in deceptive acts and practices, and that the franchisor permitted and participated in gathering consumer information in a manner that resulted in significant risk of harm. Not only is *Aaron's, Inc.* the first case that held a franchisor liable for franchisee conduct involving breach of consumer privacy, it also imposes an obligation on a franchisor to oversee and monitor the franchisee consumer privacy practices.

In this case, a number of franchisees installed privacy invasive software on the computers rented to consumers which covertly collected confidential and personal consumer information (e.g. the software logged keystrokes, captured screenshots, and activated computer webcams). The information collected was transmitted from the rented computers to franchisee email accounts. Importantly, even though the software was not used in corporate stores, the FTC concluded that the franchisor was liable for knowingly assisting its franchisees because the franchisor: (i) was cognizant that the franchisees were using the software and the franchisor's corporate server was used to store the information; (ii) allowed franchisees to access the software through its network; (iii) required its franchisees to use company provided email addresses to which the information was transmitted; and (iv) provided franchisees with vital technical support for the software.

The Privacy Commissioner of Canada ("Canadian Commissioner") took a different approach with Canadian franchisees. On August 24, 2012, the Canadian Commissioner initiated a complaint against a franchisee using the privacy invasive software. While it concluded that the franchisee contravened the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"),[2] the Canadian Commissioner did not take action against the franchisor. Following the investigation, the Canadian Commissioner provided a copy of its decision to other Canadian franchisees that it had reason to believe may have been using the privacy invasive software.

Wyndham[2]

Following three consumer data security breaches on computer systems maintained by franchisees of the Wyndham Group, the FTC filed a complaint against the Wyndham Group of franchisors ("Wyndham" or the "franchisor") alleging that the franchisor engaged in "deceptive" practices by (i) misrepresenting that it implemented "industry standard practices" and (ii) that it used "commercially reasonable efforts" to protect personal information against unauthorized access. Moreover, the FTC alleged that the failure to maintain reasonable data security measures constituted "unfair" practices and Wyndham was responsible for creating information security policies and programs for its franchisees.

Further momentum was created by the recent decision of the U.S. District Court (for the District of New Jersey)[4] to deny a motion to dismiss the FTC complaint against Wyndham on the basis that the franchisor should not be held responsible for the consumer data security breaches taking place on systems maintained by the franchisees.

Some important facts of the case include the fact that Wyndham's franchisees were contractually required to purchase a designated property management system which had to be configured to Wyndham's specification. The property management system was used for hotel reservations, check in and check out procedures, room assignment and inventory management, and to process payment card transactions. The property management systems stored personal information about guests and was part of the central reservation system maintained and managed by Wyndham (which had exclusive administrator access and rights). Franchisees paid fees to the franchisor to support and service their property management systems.

Between April 2008 and January 2010, there were three incidents of cyber-attacks on franchisee property management systems resulting in consumer data security breaches. The FTC claims that more than 619,000 consumer payment card account numbers were accessed resulting in more than $10.6 million in fraud. The FTC claims that the breaches resulted from Wyndham's failure to maintain reasonable cybersecurity measures for consumer data stored on both the franchisor and franchisee systems.

Interestingly, while the court rejected arguments that the breaches occurred solely at the franchisee system level, it concluded that it could not make a determination at the stage of the motion to dismiss that there was, as a matter of law, a distinction between the franchisor

maintained computer systems and practices and those maintained by the franchisee. More concerning is the comment made by the court that a consumer would not appreciate such distinction. It will be interesting to watch how this case unfolds.

For practical steps in developing an information governance program, see Navigating the Cyber Liability Storm – Part II.

[1] *Aaron's, Inc.*, 122 FTC 3264 (2014) (Docket No. C-4442)
[2] SC 2000, c 5
[3] *Federal Trade Commission v Wyndham Worldwide Corporation*, No. 13-cv-01887, (U.S. District Court of New Jersey, April 7, 2014)
[4] Ibid

FOR MORE INFORMATION CONTACT:

Andrae J. Marrocco is of Counsel in Dickinson Wright's Toronto office. He can be reached at 416.777.4046 or amarrocco@dickinsonwright.com.