FRANCHISE & DISTRIBUTION

NAVIGATING THE CYBER LIABILITY STORM – PART II

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 (*Aaron's, Inc.*[1] and *Wyndham*[2]) have raised awareness of the risky climate for franchisors in the realm of cybersecurity and privacy compliance. For a summary of these cases see *"Navigating the Cyber Liability Storm – Part I."*

Weathering the storm

In light of the *Aaron's*, Inc. case (notwithstanding the Privacy Commissioner of Canada's decision not to pursue franchisors) and the *Wyndham* case (which is yet to be finally determined), it would be wisdom of the most doubtful kind that would prevent franchisors from taking immediate action to develop information governance programs to protect their brands from potential data security breach liability.

Understandably (and yet in this case ironically), franchisors typically refrain from interfering with franchisee level operations (including as in this case providing services and guidance on matters such as cybersecurity) for risk of liability. This is part of the delicate balancing act that franchisors face in protecting their brand while avoiding direct and vicarious liability. Add to this the fact that addressing information governance across a franchise system is complex, time consuming and costly, and no governmental authority or court has to date offered guidance on how franchisors should develop information governance programs.

However, those issues and concerns are outweighed by the following factors that militate in favour of the franchisor taking action with respect to cybersecurity and information governance: (i) first and foremost, the reputational harm and economic impact of addressing cyber-attacks can be formidable (one study put the average financial expenditure in dealing with after effects at $5.5m); (ii) franchisees do not have the necessary financial or human resources to develop and maintain appropriate information governance programs on their own; (iii) it is apparent from the cases above that the computer systems of franchisees and franchisors are often interconnected, making cybersecurity a joint responsibility; (iv) the cases articulate an obligation imposed on franchisors to create cybersecurity policies and programs for franchisees and to oversee and monitor their practices; and (v) taking a proactive approach in developing robust policies and procedures and monitoring compliance will provide increased protection against cyber-attacks and will also provide a defence in circumstances of data security breach liability.

Practical steps

Franchisors should take the following steps in developing their information governance program.

Invest human capital. The best intentions will not develop or implement a robust information governance program. Franchisors need to dedicate the requisite human resources to the project by identifying people that are responsible for data management and privacy compliance, complement as necessary (perhaps with management level officers), and assemble a functional project team to address information governance.

Audit and risk assessment. Undertake a review of existing policies and procedures with respect to information governance together with current practices relating to the collection and maintenance of data and cybersecurity. Take time and care to identify vulnerabilities, and potential risks; Canvass and consider alternative industry practices (including current hardware and software applications used).

Develop an information governance program. This is an expansive project. It incorporates the entire process by which the franchise system collects, uses, stores and ensures the security of data (including the approach to privacy and data compliance). Part of the program will involve determining the apportionment of financial and practical responsibilities between the franchisor and the franchisee. In certain circumstances, it may be justifiable for the franchisor to impose a fee for services provided as part of the program (e.g. in setting up systems for the franchisees).

Training and monitoring. Determine the appropriate level of training required and whether such training will be provided internally or outsourced. The same consideration applies to monitoring of the information governance program. Organizing external training/ monitoring periodically provides opportunity to have ongoing independent assessment of your information governance program. It is critical that franchisees are provided with all possible resources to ensure the success of the program.

Compliance. Include in the franchise agreement a provision requiring compliance and commitment to the information governance program (referenced as being part of the operating manual). The details of the program should be included in a separate chapter or segment of the operating manual to allow for more efficient and practical updating.

Updating. Given the increasingly rapid pace at which technology continues to advance, and the sophistication of cyber-attacks, the information governance program should be reviewed and updated on a regular basis. Undoubtedly, policies, procedures, systems, hardware, software etc will require updating across the franchise system.

---

[1] Aaron's, Inc., 122 FTC 3264 (2014) (Docket No. C-4442)

[2] Federal Trade Commission v Wyndham Worldwide Corporation, No. 13-cv-01887, (U.S. District Court of New Jersey, April 7, 2014)

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.