EXPERT ADVICE

Key Privacy and Security Issues for Franchisors

By David Katz and Bess Hinson

David Katz is a partner with Nelson Mullins Riley & Scarborough LLP (Atlanta) where his practice focuses on regulatory compliance, consumer privacy and data security compliance, information governance, ethics, corporate governance and enterprise risk management. Bess Hinson is an associate with Nelson Mullins Riley & Scarborough LLP (Columbia) where her practice focuses on all stages of data incident response, including investigation, notification, remediation, managing privacy class action risks and defense of litigation and regulatory inquiry. david.katz@nelsonmullins.com, bess.hinson@nelsonmullins.com.

Franchises remain among the most highly targeted business type for cyber-criminals. A cyber-attack on a franchisee can trigger a complex forensic investigation and can be a no-win situation for the franchisor. Theft of consumer payment and proprietary data can damage a brand financially and destroy the brand's reputation among its consumers. The brand faces the negative impact across the entire system for a data breach at a specific location, the franchisee. As a smaller business, the franchisee may find it difficult to make the necessary investments and keep up with all the requirements, laws, contractual obligations and best practices concerning data security. And yet, the FTC and consumers are pursuing franchisors for franchisee breaches or inadequate security practices with increasing frequency. Determining the best course of action to address these risks requires careful consideration and a complete analysis of the legal and business decisions required to fully remediate or minimize these risks.

Why This Matters

Many franchisors have been hesitant to implement specific requirements or even provide franchisees with significant guidance on data security and PCI compliance due to the concern that doing so would increase the risk of a liability finding if a data breach occurred, even though the franchisee is a separate legal entity. However, in the case of data security and PCI compliance, there are several countervailing reasons why franchisors need to consider greater involvement in these specific issues:

1. To protect the brand. Consumers may not distinguish between independently owned franchises and the brand so a data breach at one location can have detrimental impact across the entire brand.

2. Franchise systems use an interconnected computer network to varying degrees, allowing sophisticated hackers to expand the target upon entry at one location. In some instances, franchise systems may supply the networking infrastructure and technology components to the franchisees. One franchisee can be the weak link that allows a breach to occur across the network.

3. With respect to regulators and some claims for vicarious liability, a franchisor's implementation of policies and requirements for data security may provide a defense.

4. Through training, monitoring and auditing, the franchisor may mitigate some risk to the franchise system.

5. Franchisors should consider fully disclosing the areas of shared exposure and risk related to data security and ensure the Franchise Disclosure Document is clear with respect to these risks.

6. The parties can allocate the respective responsibilities for achieving and maintaining PCI compliance, data security and provide other protections in the franchise agreements.

Notably, in June 2012, the FTC alleged a Section 5(a) claim against a hotel franchisor for a data breach. The FTC alleged that, due to security failures, intruders

could break into a franchisee's system, and from there access the corporate system, ultimately resulting in over half a million payment card accounts being compromised and almost $11 million in fraud loss. The lesson here is that the FTC is more likely to target franchisors that fail to require adequate data protection policies and procedures for their franchisees. The settlement agreement between the FTC and the hotel franchisor mandates a twenty-year requirement to, among other things, maintain a comprehensive information security program including annual certified third party risk assessments and mandated breach response measures in the event of future breaches. The settlement agreement imposes substantial reporting and compliance requirements on the hotel franchisor and will require significant investment for the future in order to comply with the settlement terms. The bottom line is the risk to the brand of liability to third parties and government regulators suggests that franchisors should be ensuring franchisees are PCI compliant and undertaking defensible data security protection measures.

Strategy for Franchisor Cybersecurity Preparedness

Below is a list of what a franchisor's legal advisor should be in charge of handling:

• Perform a data security risk assessment of the franchisor and franchisees under the attorney-client privilege and map the data flows of the franchise system. They need to assess systems for security, PCI compliance, firewall protection, POS system selection, retention and destruction of customer information, payment data encryption and consumer facing privacy policies. We identify gaps and recommend tailored remedial steps based upon the laws applicable to the franchise system.

• Advise the franchisor on language for inclusion in the Franchise Disclosure Document to address privacy and data security obligations on the part of the franchisees and for franchisor systems or technologies franchisees are required to purchase, lease or access during the term of the franchise agreement.

• Advise the franchisor on whether the existing franchise agreement executed by the parties addresses privacy and data security compliance, ownership of customer data, training of franchisee employees regarding the use of the technology services, cyber liability insurance and incident response obligations in the event of a breach, in addition to who bears the burden of costs associated with privacy and data security protection and compliance.

• Advise on the role the franchisor should play in oversight, audit and enforcement of franchisees' privacy and data security policies and can assist franchisor in the development of these audit and enforcement programs.

• Develop franchise agreement provisions that give the franchisor more control over post-breach issues. For example, these provisions require notice to the franchisor upon detecting a breach; provide for sufficient cooperation with the franchisor, including access to the franchisee's IT systems, to halt the attack and conduct an investigation; the right to name legal counsel and control the media communications regarding the issue, including a covenant by the franchisee not to make any public statements about the breach without the franchisor's approval.

• Assess whether a franchisor should set out its own data security standards and audit schedules in the franchise agreement or require compliance with third-party standards and audits.

• Review and update commercial contracts with third parties providing services under the franchise system (for example, POS vendors) to ensure consistent and proper protection in light of the types of data involved. Address privacy concerns in all vendor agreements.

• Help the franchisor navigate indemnity issues for costs and claims associated with a data breach, with the goals of shifting costs of the response to the responsible franchisee.

• Advise on the development of network security guidelines for franchisees.

• Develop data security training procedures for franchisees and connect franchisors to trusted partners, such as information security vendors and other information security professionals that can advise the franchise community.

• Develop standard privacy policies and other regulatory-required data security procedures and programs for franchisees. We develop user-friendly guidance to help franchisees understand their obligations under these policies, so that practices are consistent across the franchise.

• Develop a standard cybersecurity incident response plan for all franchisees, and a response plan for the franchisor in how to manage a franchisee's breach incident.

• Where applicable, they should develop a comprehensive information security program designed to protect cardholder data – including payment card numbers, names and expiration dates.

Unfortunately, there is no easy fix to these issues and one approach may not be appropriate in all circumstances. The best way to prepare is to understand that each franchise system has its own features, culture, risk tolerances, business systems, methods of operation, information technology infrastructure support systems, marketing and promotional practices and data collection and sharing practices. However, any franchisor can begin to assess potential exposure, and take steps to identify and mitigate risk to the franchise system.