Cyber Security and Protecting Franchise System Customer Data

As you know, data and privacy protection and cyber security have become increasingly problematic, with news of privacy or data breaches at large retailers a somewhat regular occurrence. But it is not just Target or Neiman Marcus. Recently, the restaurant chain P.F. Chang's notified customers of a data breach involving its customers' credit and debit cards. And, as we reported on the Wyndham hotel case in April, the FTC is seeking to hold Wyndham liable, *as franchisor,* due to the data and privacy breaches in its system which occurred at franchised hotels. As long as there is value in obtaining customer data, cyber thieves will continue to hack into systems.

As a franchisor, your concerns are multiplied because the data collected throughout your system is vulnerable from multiple entry points—each franchisee office, each franchisee location, and each computer terminal or POS at a franchised location; the computer terminals and POS at each company-owned or affiliate-owned outlet; your corporate headquarters; and all of the vendors to your system. With the FTC's stepped-up enforcement (or at least its public statements to that effect), and the recent court decision that suggests that a franchisor is liable, or should be liable, for data or privacy breaches that occur at a franchised location, you may be wondering what to do.

There is no easy fix, or silver bullet, for this burgeoning problem. And each franchise system has its own features, business systems, methods of operations, computer systems and data collection practices. However, you can begin to assess your potential exposure, and take steps to mitigate risk. The following are our suggestions, based on recent court decisions, FTC consent decrees, reported data breaches, and our work with clients on cyber security, privacy and data matters.

1. Review your website privacy policy and terms of use, and make sure that they are accurate and consistent

In the Wyndham case, the court found that a reasonable consumer might have understood that the Wyndham privacy policy covered data security practices at both company-owned and franchised hotels due to conflicting or inconsistent statements in the policy. You should confirm that any factual statements and disclaimers in your policies are not arguably contradicted by other parts of the policies.

2. Perform a data privacy and security compliance audit

You should analyze the process by which customer data is collected, stored, accessed, shared and controlled by the franchisor and your franchisees, and the extent to which information on this process is communicated to customers. The audit should consider the policies, procedures, and practices that are necessary for your business, relative to the collection, use, and sharing of personal information. Also, depending on the nature, scope and geographical reach of your system, you should determine which federal, state, and international laws apply. Finally, you should evaluate the appropriateness of your policies and procedures and whether they follow best practices.

3. Follow reasonable and appropriate measures for securing customer data

Consider both administrative and technical safeguards. If you do not have the capabilities in-house (or even if you do), consider retaining an outside consultant to provide guidance and recommendations.

4. Address privacy concerns and requirements in all vendor agreements

Review vendor agreements to confirm that they address data privacy and security issues. The Target data breach was the result of an HVAC vendor's lax protection of its password credentials, which ultimately allowed the unauthorized access to the Target point of sale system.

5. Make sure you have a data breach response plan in place

Do not wait until you have a data breach to take action. Appoint a person or team responsible for handling any data breach and have in place a process for dealing with breaches. Legal counsel, upper management, IT, public relations, and employees must all be included in the plan and process.

6. Provide ongoing training

Data privacy and security can be easily compromised by lax employees (and management) who are not sufficiently trained in the data privacy and security policies and procedures of a business. Employees who do not follow procedures can be the weak link, or unlocked door, for cyber pirates and phishing expeditions. Therefore, conducting training—for franchisees and franchisor employees—is necessary. (See our comments below in #8, regarding franchisee training.)

7. Consider available cyber insurance

New forms of cyber insurance are available to mitigate risk of a data breach, but these should be scrutinized for value and coverage. Traditional commercial business insurance is generally insufficient for cyber risks largely due to a variety of exclusions. Franchisors can obtain cyber insurance, and franchisors can require that their franchisees obtain cyber insurance. While most franchise agreements do not specifically identify cyber insurance as a required coverage, many franchise agreements contain provisions that permit a franchisor to modify the insurance requirements over time based on changes in the industry, the marketplace or risks.

8. Franchisors should require that franchisees become knowledgeable about the risks, and impose certain equipment, software, and/or vendor requirements at the franchisee level to minimize exposure

Franchisees will look to franchisors for guidance in this area. And franchisors should provide assistance–to help franchisees and to protect the system and network. Therefore franchisors should conduct training to make sure that franchisees are aware of best practices. To reduce exposure to vicarious liability claims, franchisors may require that franchisees participate in third-party or industry association sanctioned training programs, and certify to the franchisor that the franchisee, its management and staff have completed training and implemented data security safeguards. As with many other areas of franchisee operations, a franchisor walks a narrow line between, on the one hand, providing advice, guidance and assistance, and even imposing requirements, to protect

the brand and system from problems or missteps that might occur at the franchised outlets, and, on the other hand, crossing over the line to becoming overly involved in franchisee operations, which heightens the risk of vicarious liability claims.

* * * * *

We expect to see more instances of attempted, and successful, hacking and theft of customer data from large and small chains, and with it will come consumer complaints, federal and/or state actions, and negative press. We also expect to see Congressional action to try to develop a more comprehensive and unified national standard for data security and breach notification. But, franchisors must take the first steps to protect their brand and their systems, and help their franchisees. The old adage applies here: you are only as strong as your weakest link.

If you would like us to provide more detailed analysis of your system's privacy and data security controls, including conducting a data and security compliance audit, reviewing privacy policies, or analyzing insurance coverage, please contact us. Also, we are considering conducting a webinar on cyber security and data privacy for franchise systems. If you and/or your colleagues would be interested in such a webinar please let us know.

Finally, we have recently co-authored "A Legal Guide to Privacy and Data Security," which is a collaborative effort of the Minnesota Department of Employment and Economic Development and GPM, and contains information on state and federal data security laws. A hard copy is available from us, at no charge, or you can download a copy from our website.

If you have any questions, please contact us.

Jennifer Debrow
Principal, Co-Chair of Privacy Team
612.632.3357
jennifer.debrow@gpmlaw.com

Brian Dillon
Principal, Co-Chair of Privacy Team
612.632.3313
brian.dillon@gpmlaw.com