Duff on Hospitality Law

FTC v. Wyndham: Recent Action

07.20.12 01.07.26

Last month the Federal Trade Commission filed a lawsuit against Wyndham Worldwide Corporations and three of its subsidiaries ("Wyndham") in U.S. District Court in Arizona. The complaint alleges that Wyndham engaged in unfair and deceptive practices by failing to implement reasonable data security protections on computers used by independently owned Wyndham hotels and because the company's public privacy policy misrepresented the security measures it actually employed to protect customer's personal information. Specifically, the Commission alleged that Wyndham:

- failed to use strong (and in some cases any) passwords to limit access to computer files;
- failed to use firewalls to separate corporate and hotel computer systems;
- improperly stored payment information in clear text;
- failed to implement reasonable measures to detect security breaches;
- failed to implement proper incident response procedures or remedial steps after learning of a data breach; and
- failed to adequately restrict access to company systems by third party vendors.

The claims stem from three separate data breaches over a period of two years in which hackers obtained the private information of more than 600,000 customers, which led to more than $10.6 million in fraudulent charges.

Of course, this is not the first case brought by the FTC relating to consumer privacy. The FTC has initiated more than 32 data privacy and security enforcement actions since 2002; however, this case is important for several reasons:

- Defendant's Industry and Business Model: The food and beverage industry (including hospitality) accounted for 51.6% of the data breach investigations in 2011. Making matters worse, franchise models like Wyndham's accounted for more than a third of the 2011 investigations, which continues a trend that began in 2010. So, it is likely that the FTC will continue to target hotels and hospitality franchises in the future.
- Exposure: There is a lot of money involved. Putting aside the potential cost of litigation (fines in these types of FTC actions often exceed several million dollars, with the recent Google settlement coming in at $22.5 million), the more than $10 million in fraudulent charges, and the harm to Wyndham's reputation, the cost of responding to data breaches of this sort are staggering.
- Timing: This is one of the first actions the FTC brought after it recently released its final report and recommendations on consumer privacy and security, "Protecting Consumer Privacy in an Era of Rapid Change" ("Privacy Report"). Among other things, the Privacy Report recommends "clearer, shorter, and

more standardized" privacy policies that will allow consumers to understand and compare privacy practices, expands the scope of protected information to include any data that may be linked to a consumer, computer or device, and directs companies to "de-identify" consumer data and contractually prohibit downstream entities from attempting re-identify it.

- Downstream Responsibility: The Complaint includes claims for activities of down stream users. Although the complaint alleges that Wyndham controlled the activities of the franchise hotels through its franchise and management agreements, the fact remains that even if this had not been the case Wyndham would have been responsible. The FTC has long taken the position that a company in Wyndham's position will be responsible for the privacy practices of not only its affiliates and suppliers, but its customers as well. *See SettlementOne Credit, File No. 082-3208 (FTC Feb 3, 2011)*. As the recommendations in the Privacy Report indicate, this includes an obligation to ensure that third-party contractors with whom the company deals have adopted and comply with adequate privacy and security measures.
- Claims: The complaint asserts both deception and unfairness claims and, in accord with the Privacy Report, suggests that the latter may be met even if there is no tangible harm to consumers. This represents a departure, since unfairness has been traditionally applied only where there is (a) substantial consumer injury (interpreted as a tangible injury), (b) the injury is not outweighed by countervailing benefits and (c) the injury is not reasonably avoidable by the consumer.
- District Court: The FTC filed suit in U.S. District Court. Typically, the FTC settles these cases via consent orders, most completed before a complaint is filed. So, this case may present an opportunity for the court to weigh in on the "standards" developed over the years for protecting consumer information.

Given what the FTC suit reveals about its priorities, hospitality industry members should be even more vigilant about data privacy and protection issues. Here are some steps you should consider to reduce the likelihood of a claim:

- Review your privacy and data security policies and practices frequently and regularly to be sure that they conform to changing expectations of the public and regulators. Unlike health care providers and financial institutions, companies in the hospitality industry are not generally subject to legislation mandating specific data privacy and security standards so for the most part, your actions will be analyzed in reference to unwritten and continually evolving "industry standards," and an unfairness principle described by FTC Commissioner J. Thomas Rosch as an "elastic and elusive concept." As concerns for consumer privacy increase, the standards by which a company's practices are measured will inevitably become stricter. For example, data breach requirements were virtually non-existent just a few years ago and are now almost ubiquitous.
- Review the FTC complaint against Wyndham for guidance as to what is expected, and what not to do and take corrective measures where needed. Likewise, review the recommendations in the Privacy Report, since these offer a preview of what is on the horizon. At a minimum, have and disseminate throughout your organization as appropriate a written information security policy and breach response plan, do what you say you will do in your consumer-facing privacy policies, follow industry best practices, and take any specific steps suggested or listed in the above FTC materials. You might also consider Trustwave's "

Security Alert for Businesses in the Hotel, Motel and Lodging Industries" and "Five Security Issues All Hotel Operators Need to Know", Tia D. Ilori, Hospitality Upgrade, Spring 2011.

- Remember, you are also responsible for the policies of your contractors, vendors, downstream distributors and any other third-party with access to your customer's data or even your systems. Consider developing standard contracts that address data security and privacy obligations, and make third parties responsible, including via warranties for compliance and indemnities in the event of claim, and purchase insurance against the cost of data breach.
- Identify those elements of the security matrix that you can competently handle and those that should be outsourced. Hospitality companies are not always expert in all aspects of their business, and when it comes to security and privacy, the best course may be to hire it out (with the proper contracting language, as discussed above).

In short, the FTC's complaint against Wyndham serves as a wake-up call: until applicable privacy standards are legislated or approved by the courts, companies in the hospitality industry, perhaps more than most, need to be particularly diligent in their efforts to meet the requirements of that "elastic and elusive concept" known as fairness by which their efforts will be judged.

If you have questions or would like additional information about this topic, please feel free to contact Greg.

Posted in Data Privacy

Tagged as Data Breach Report, Federal Trade Commission, FTC Act, Global Security Report, Privacy Report, security enforcement actions, Wyndham Worldwide Corporations