Wyndham Hits a Wall in Challenge to FTC Data Breach Authority

Alysa Z. Hutnik

April 11, 2014

Earlier this week, a federal district court in New Jersey issued an opinion ruling on Wyndham Worldwide Corporation's and three of its subsidiaries' (collectively "Wyndham's") motion to dismiss, finding for the FTC on all grounds. While the court noted that the "decision does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked," the opinion underscores the risk exposure for companies that incur a data breach (or otherwise collect/store consumer data), and face FTC scrutiny thereafter as to whether their information safeguard practices are consistent with FTC expectations. While the FTC has reached over 50 data security settlements, this case represents the first time that the FTC is litigating its theory that a business's privacy and data security practices may be unfair and/or deceptive under Section 5 of the FTC Act.

Background

On June 26, 2012, the FTC filed a lawsuit against Wyndham. The FTC alleged that the companies engaged in unfair and deceptive practices and violated Section 5 of the FTC Act by failing to implement adequate data security protections on computer systems located at 90 independently-owned Wyndham-branded hotels with which the Defendants maintained franchise agreements.

The complaint alleged that the Defendants' failure to implement reasonable and appropriate data security safeguards at the franchisee locations allowed computer hackers to breach franchisee computer systems and the Wyndham hotel data center on three separate occasions between April 2008 and January 2010. The hackers were able to gain access to the financial account information for more than 600,000 hotel customers. The FTC's complaint also claims that Wyndham's privacy policy misrepresented the extent to which the company protected consumers' personal information. The complaint sought injunctive relief to prevent future violations of the FTC Act, as well as monetary relief for the affected hotel customers.

Wyndham's Motion to Dismiss

In April 2013, Wyndham filed a motion to dismiss, seeking to dismiss the FTC's complaint on four grounds. First, Wyndham challenged the FTC's authority to assert an unfairness claim in the data-security context. Second, Wyndham asserted that the FTC must formally promulgate rules or regulations before bringing an unfairness claim, and by failing to do so, the FTC is violating fair notice principles. Third, Wyndham argued that the FTC's allegations are plead insufficiently to support either an unfairness or deception claim. Lastly, Wyndham challenged the FTC's deception claim that Wyndham's privacy policy misrepresented measures taken by the company to protect consumers' personal information.

Ruling on Motion to Dismiss

On April 7, 2014, the court issued an opinion, *FTC v. Wyndham Worldwide Corporation, et al.*, No. 13-1887 (D.N.J., Apr. 7, 2014) (Opinion), ruling on Wyndham's motion to dismiss, finding for the FTC on all grounds.

In challenging the FTC's authority to assert an unfairness claim in the data-security context, Wyndham argued that Congress has passed narrowly tailored data security legislation – including the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Children's Online Privacy Protection Act – and that the overall statutory landscape does not authorize the FTC to generally establish data security standards for the private sector under Section 5. The court disagreed, stating that the FTC's unfairness authority over data-security can coexist with the existing data-security regulatory scheme. In addition, the court found that data-security legislation proposed by Congress and the FTC's public representations that it lacks the authority to require entities to adopt privacy policies, do not give rise to a data-security exemption from the FTC's unfairness authority.

Wyndham also asserted that the FTC would violate basic principles of fair notice and due process without promulgating rules, regulations, or guidelines explaining what data-security practices the Commission believes is required under Section 5. Wyndham argued that the FTC's prior consent decrees and its business guidance provide no such guidance. The court, however, was not persuaded by these arguments. The court recognized that previous Circuit Courts of Appeal have affirmed FTC unfairness actions in a variety of contexts without preexisting rules or regulations specifically addressing the conduct-at-issue. The court was also unpersuaded that regulations are the only means of providing sufficient fair notice. The court stated that Wyndham's "argument that consent orders do not carry the force of law…misses the mark." Indeed, the court found that FTC's rulings, interpretations and opinions, while not controlling upon the courts, do constitute a body of experience and informed judgment to which courts and litigants may properly resort for guidance.

Wyndham further argued that an unfair practice must, by statute, cause consumer injury, and that injury from theft of a payment card data is never substantial and always avoidable. The court, however, found that FTC's complaint sufficiently plead an unfairness claim under the FTC Act. Importantly, the court stated that the FTC's allegations permit it to reasonably infer that Wyndham's data-security practices caused theft of personal data, which ultimately caused substantial injury to consumers.

Lastly, in finding that the FTC's deception claim was sufficiently plead, the court turned to the specific language found in Wyndham's privacy policy. Wyndham argued that its privacy policy specifically excludes Wyndham-branded hotels from the policy's data-security representations. The court was not convinced, noting that a reasonable customer would have understood that the policy makes statements about data-security practices for both Wyndham and Wyndham-branded hotels.

* * *

Although the court's ruling confirms that the FTC has the authority to assert an "unfair" or "deceptive" claim in the data-security context, the case will continue to be litigated on the issue of whether Wyndham's data security practices constituted a violation of Section 5 of the FTC Act. In the meantime, companies can help protect themselves by reviewing their information collection and security practices, carefully evaluating the type of information collected from customers or users of its websites, confirming that all data collected is transmitted and stored securely, and ensuring that all privacy and data-security representations accurately describe the practices.