crowell moring

CLIENT ALERT

Wyndham Decision Upholds FTC Authority to Regulate Data Security

Apr.08.2014

In a much-anticipated decision, the U.S. District Court for the District of New Jersey upheld the FTC's authority to regulate data security practices by denying Wyndham Worldwide Corporation's motion to dismiss challenging the FTC's authority to pursue unfair and deceptive trade practices claims arising from a cyber breach. The complaint against Wyndham asserts that Wyndham's data security policies constituted unfair and/or deceptive trade practices, prohibited by Section 5(a) of the FTC Act, codified here. This is only the second challenge to the FTC's data security regulatory authority under Section 5 in federal court. In the first, *FTC v. Accusearch,* the 10th Circuit supported the FTC's authority under Section 5 of the FTC Act.

Recent Happenings in APRM
April 2014

- Wyndham Decision Upholds FTC Authority to Regulate Data Security
- District Court Allows Class Action Lawsuit over '100% Natural' Claims to Proceed
- NHTSA Finalizes Rule Requiring New Vehicles to Possess Rear Visibility Technology
- Draft List of Priority Products Announced for California's Safer Consumer Products Program

Wyndham and its subsidiaries own and manage franchised Wyndham hotels throughout the United States. From 2008–2010, hackers, allegedly operating out of Russia, gained unauthorized access to Wyndham's computer network and to the property management systems of individual hotels, on three separate occasions. According to the complaint, the hackers accessed over half a million unique payment card accounts, along with their associated names and security codes. These account numbers were exported to a domain registered in Russia. Fraudulent charges on the compromised card accounts totaled over $10 million. The FTC filed its complaint on June 26, 2012, alleging that Wyndham's failure to enact reasonable data security policies constituted an unfair trade practice, and that its published online privacy policy was "deceptive."

Wyndham challenged the FTC's authority to regulate data practices under Section 5. First, Wyndham argued that the FTC lacked authority under the unfairness prong of Section 5(a) of the FTC Act to regulate data security practices. Wyndham argued that the existence of other data security regulations as well as the FTC's past statements disclaiming any authority over data security practices precluded the FTC's claims. Judge Salas disagreed, holding that "the FTC's unfairness authority over data security can coexist with the existing data-security regulatory scheme." Further, she noted that "even accepting that the FTC shifted its stance on data security, this cannot limit its authority without more."

Next, Wyndham argued that "it would violate basic principles of fair notice and due process" to allow the FTC to regulate data security practices under the unfairness prong without promulgating rules explaining how it intended to do so. The court disagreed, observing there is no requirement for the "FTC to formally publish a regulation before bringing an enforcement action under Section 5's unfairness prong."

Finally, Judge Salas ruled that the consumer injuries alleged in the complaint were both substantial and not reasonably avoidable. Notwithstanding the federal limit of $50 for consumer liability for unauthorized use of payment cards, the court

found that the allegation of misuse of the hacked payment card data sufficed for the purposes of surviving a motion to dismiss. Similarly, the court found Wyndham's argument that consumers could potentially avoid injury by seeking remuneration from their card issuers required an analysis that was too fact-dependent to grant a motion to dismiss.

Concerning the FTC's deception claim, Wyndham argued that the FTC's complaint lacked merit because the Wyndham-branded hotels and the company, Wyndham Hotels and Resorts, LLC, are legally separate entities, and in any event, the company's privacy policy expressly disclaimed any representations as to the data security practices of the Wyndham-branded hotels. Judge Salas rejected the argument that Wyndham and Wyndham-branded hotels are separate entities for the purpose of the complaint. She also ruled that Wyndham's disclaimers did not effectively communicate its privacy policy to consumers.

This case essentially leaves undisturbed the FTC's authority under Section 5 to regulate data practices and investigate data breaches. The FTC has investigated multiple data security matters, and FTC Commissioners have underscored the high priority the Commission places on vigorous enforcement to protect consumers from data security breaches. In past cases, FTC enforcement has resulted in consent orders that call for improvements in privacy protection, oversight of privacy policies, privacy audits and fines that have been as high as $35 million.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jeffrey L. Poston
Partner – Washington, D.C.
Phone: +1 202.624.2775
Email: jposton@crowell.com

Christopher A. Cole
Partner – Washington, D.C.
Phone: +1 202.624.2701
Email: ccole@crowell.com

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com