Recent Appellate FTC Cybersecurity Ruling

Jeffrey S. Jacobovitz and Eric D. Olson

On August 24, 2015, the United States Court of Appeals for the Third Circuit ruled that the Federal Trade Commission (hereinafter "FTC")[1] has the power under the FTC Act to police companies that fail to employ adequate security and privacy practices to protect the information of their customers. Since 2005, the FTC has brought administrative complaints against companies with allegedly deficient cybersecurity practices, but the vast majority ended with a settlement or consent order.

This case was the first in which an appellate court considered the FTC's ability to bring suit under Section 5, 15 U.S.C. § 45 (a)'s prohibition on "unfair or deceptive acts or practices in or affecting commerce" based on inadequate cybersecurity practices. In its lawsuit against Wyndham Worldwide Corporation and related companies, the FTC sought to hold the hotel franchisor and owner liable for three data breaches in 2008 and 2009, when hackers stole credit card and other information from about 619,000 consumers. This led to $10.6 million in unauthorized charges. Wyndham's 15 hotel brands include Days Inn, Ramada, Travelodge, Microtel Inn & Suites, and Planet Hollywood.

Background

The FTC had alleged that Wyndham engaged in seven specific cybersecurity practices that together exposed consumers' personal data to unauthorized access and theft, including, among others, permitting its hotel chains to store payment card and other information in clear readable (unencrypted) text, failing to utilize firewalls or limit access to its corporate network from the internet, and permitting its hotel chains to use default and easy-to-guess user accounts and passwords. Together, the FTC argued that these and other inadequate practices constituted "unfair or deceptive acts or practices in or affecting commerce" under Section 5. The FTC also filed a deceptive practices claim alleging that Wyndham overstated its cybersecurity practices on its website. When Wyndham moved to dismiss both claims, the United States District Court for the District of New Jersey denied the motion, but certified Wyndham's unfairness claim for interlocutory appeal.

Wyndham responded with a series of arguments why the cybersecurity-based claims brought by the FTC did not fall within the bounds of "unfair" conduct under Section 5, including that the cybersecurity-related claims brought by the FTC fell outside the plain meaning of the statute, that subsequent congressional action reshaped Section 5 to exclude cybersecurity, and that the FTC's own attempts to obtain broad cybersecurity enforcement powers from Congress demonstrated that it lacked such authority. The hotel franchisor also contended that it did not receive fair notice of the specific cybersecurity standards the FTC would require it to meet, arguing that it was entitled to "ascertainable certainty" of the FTC's interpretation of Section 5's application to cybersecurity.

In his opinion for the unanimous three-judge panel, Judge Thomas Ambro rejected each of these arguments. He wrote that Wyndham had failed to demonstrate that Wyndham's "alleged conduct falls outside the plain meaning of 'unfair'" under § 45(a). In so doing, the panel rejected all of Wyndham's arguments. Judge Ambro wrote, in particular rejoinder to Wyndham's *reduction ad absurdum* argument that such a broad reading of § 45 (a) would grant the FTC authority to regulate hotel room door locks or "sue supermarkets that are 'sloppy about sweeping up banana peels,'" that, "were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 consumers fall hardly suggests it should be immune from liability under § 45 (a)."

1 Mr. Jacobovitz is a former attorney with the Federal Trade Commission.

The Third Circuit panel also wrote that the FTC was not required to set forth the specific cybersecurity standards that Wyndham was required to meet because the FTC is seeking judicial interpretation of the requirements of § 45 (a), not requesting deference to its own administrative interpretation of the provision. As such, the court wrote that Wyndham need only have fair notice of the requirements and meaning of the statute, and is not entitled to know with "ascertainable certainty" the FTC's interpretation of what cybersecurity practices are required by § 45 (a). The Court held that Wyndham is entitled to only a relatively low level or statutory notice, and such notice is satisfied "as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute." In view of the fact that Wyndham was hacked on three separate occasions, the court held that Wyndham was certainly on notice of the possibility that a court could find that its cybersecurity practices failed the cost-benefit analysis of § 45 (n) after the second attack.

AGG Takeaways

This case marks the first time that a federal appellate court recognized an expansion of the FTC's authority under § 45 (a) to cover unfair cybersecurity practices. As the number of data breaches and other cybersecurity attacks increase, companies face the added injury of an FTC investigation or lawsuit attacking their cybersecurity practices, on top of the costs of responding to the data breach and the loss of business that accompany a data breach. Accordingly, companies should consider investing in a review of their cybersecurity policies and procedures by experts in the law and technology of data security. Additionally, in the event of a data breach, companies should keep an eye toward potential investigations or lawsuits by both consumers and the federal government, in light of the FTC's newfound cybersecurity enforcement authority under § 45 (a). Engaging counsel with expertise in cybersecurity compliance, consumer class actions, and FTC enforcement actions should be high on the priority list of any company that collects customer payment data or personal identification information.

The case on appeal is *Federal Trade Commission v. Wyndham Worldwide Corp.*, No. 14-3514, Slip Op. (3d Cir. Aug. 24, 2015).

Authors and Contributors

Jeffrey S. Jacobovitz
Partner, DC Office
202.677.4056
jeffrey.jacobovitz@agg.com

Eric D. Olson
Associate, DC Office
202.677.4908
eric.olson@agg.com

not *if*, but *how*.®

About Arnall Golden Gregory LLP

Arnall Golden Gregory, a law firm with more than 150 attorneys in Atlanta and Washington, DC, employs a "business sensibility" approach, developing a deep understanding of each client's industry and situation in order to find a customized, cost-sensitive solution, and then continuing to help them stay one step ahead. Selected for The National Law Journal's prestigious 2013 Midsize Hot List, the firm offers corporate, litigation and regulatory services for numerous industries, including healthcare, life sciences, global logistics and transportation, real estate, food distribution, financial services, franchising, consumer products and services, information services, energy and manufacturing. AGG subscribes to the belief "not if, but how.®" Visit www.agg.com.

Atlanta Office
171 17th Street, NW
Suite 2100
Atlanta, GA 30363

Washington, DC Office
1775 Pennsylvania Avenue, NW
Suite 1000
Washington, DC 20006

To subscribe to future alerts, insights and newsletters: **http://www.agg.com/subscribe/**