3rd Circ. Writes A Road Map For Cybersecurity Practices

Published in *Law 360*, New York (August 26, 2015, 5:56 PM ET)


Tracy E. Miller


Lisa A. Christensen

In its much-awaited Aug. 24 decision in *FTC v. Wyndham Worldwide Corp.*,[1] the Third Circuit upheld the authority of the Federal Trade Commission to regulate cybersecurity practices under Section 5 of the Federal Trade Commission Act.[2] The court decisively rejected the two principal arguments asserted by the Wyndham: (1) that the FTC lacks authority to enforce cybersecurity standards as unfair conduct prohibited by Section 5; and (2) that Wyndham did not have fair notice of the standards to which it would be held.

The Third Circuit decision allows the FTC to pursue its claims against Wyndham arising from the theft of personal and financial data for over 619,000 consumers, and sets the stage for the commission to pursue a proactive enforcement agenda against companies for substandard cybersecurity practices. The court's analysis of applicable standards for Section 5 enforcement and the discussion of specific shortcomings in Wyndham's security safeguards create a road map for companies to assess their own practices in the face of mounting security threats and clear affirmation of the FTC's regulatory authority.

Facts of the Case

In 2008 and 2009, hackers accessed Wyndham's computer systems, leading to over $10.6 million in fraudulent charges for affected consumers. On three separate occasions, hackers gained access to Wyndham's computer systems through the corporation's own data systems and the connected property management systems of Wyndham-branded hotels. According to the court's decision, in the successive attacks, hackers exploited weaknesses in the security systems left unaddressed following the prior attacks. The FTC filed suit in 2012 for violation of Section 5, alleging that Wyndham's conduct was unfair and that its privacy policy informing consumers that Wyndham used "commercially reasonable efforts" to safeguard identifiable information was deceptive.[3]

Challenge to FTC Authority

Since 2005, the FTC has brought numerous administrative actions asserting inadequate cybersecurity practices against major U.S. corporations, relying upon violation of the fairness standard of Section 5 as its enforcement tool.[4] Most of these actions have resulted in settlement. Wyndham chose to challenge the FTC's authority under the fairness prong of Section 5 to regulate cybersecurity practices, and asserted that its conduct did not in any event meet the standard. Before rejecting each of those arguments, the court set forth the applicable standard for FTC authority under Section 5. As codified by Congress in 1994, the FTC Act gives the FTC authority to pursue conduct as unfair if "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[5]

Among other arguments, Wyndham contended that conduct can only be unfair if it causes injury through unethical behavior and if it is "inequitable" or unjust. The court dismissed the requirement of unethical behavior as unsupported by judicial precedents, and concluded that it did not have to reach the issue of whether a practice must be inequitable because Wyndham met the standard by failing to comply with its own privacy policy, investing adequate resources in cybersecurity and exposing customers to substantial financial injury. Notably, in response to Wyndham's argument that conduct should not be deemed unfair if a company was itself "victimized by criminals," the court held that although

unfairness claims generally entail actual harm, the FTC Act expressly recognizes the possibility that actual harm is not an essential element of a claim of unfairness, leaving open the possibility of FTC enforcement based on company conduct in the absence of consumer injury. The court also pointed to the doctrine of foreseeability as a basis of liability, and noted that a company's conduct need not be the immediate proximate cause of an injury. The court reserved its most acerbic reply to Wyndham's argument that such a broad reading of the standard in this case would leave the FTC with the authority to "sue supermarkets that are sloppy about sweeping up banana peels."[6] Characterizing the argument as "alarmist," the court replied that "it invites the tart retort that, were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability under § 45(a)." [7]

The Third Circuit also rejected Wyndham's arguments that the FTC lacks authority to regulate cybersecurity because: (1) passage of the Fair Credit Reporting Act, Gramm-Leach-Bliley Act and Children's Online Privacy Protection Act reflected congressional intent not to grant the FTC authority to oversee cybersecurity under Section 5; and (2) prior FTC statements undercut its assertion of authority under Section 5 to pursue the claims against Wyndham. On the first argument, the court noted that each of the three statutes required the FTC to take specific actions, including the issuance of regulations, holding that the statutes did not undermine broader FTC authority to regulate cybersecurity. The court also dismissed Wyndham's assertion about prior FTC statements, finding that the statements recognized that the commission could not mandate practices by companies unless necessary to prevent substantial injury, but did not undermine its authority to regulate cybersecurity practices tied to the substantial injury standard.

Claim of Lack of Fair Notice

Wyndham argued that the FTC's assertion of the unfairness claim violated the Due Process Clause because the commission had not provided fair notice of the specific cybersecurity practices the company was required to meet to avoid liability. The court rejected this argument as well, finding fair notice where: (1) the company could reasonably foresee that a court could construe its conduct as falling within the meaning of the statute; and (2) FTC guidance is readily available on the commission's website in the form of consent decrees and other publications that provide insight into its standards.[8]

With respect to the first argument, the court opined that because the FTC had not issued a relevant rule or document, Wyndham was entitled only to fair notice of the general standard set forth in Section 5. While acknowledging that the standard is not precise, the court pointed to the standard set by Congress in 1994, as stated above.[9] As applied, the court concluded that Wyndham's claim was particularly weak, noting that after the company's systems had been hacked twice resulting in consumer injury, Wyndham could certainly have known that its conduct could fall within the ambit of Section 5. The court also stated that the *FTC Guidebook, Protecting Personal Information: A Guide for Business*, had been issued in 2007 and provided guidance even if the FTC did not identify the practices as required.[10]

Lessons Learned

Given the Third Circuit's reference to the FTC's guidance[11] and discussion of Wyndham practices identified as inadequate by the commission, the Wyndham case provides a useful road map for companies seeking to protect sensitive consumer information in accordance with the FTC's standards. In its posted cybersecurity policy, Wyndham claimed, among other things, that it used "industry standard practices" and "commercially reasonable efforts" to protect customers' information, including 128-bit encryption to protect personally identifiable information from unauthorized access.[12]

In the original lawsuit, the FTC alleged, contrary to this stated policy, that Wyndham:

- failed to use firewalls between networks;
- failed to encrypt stored payment card information (the information was stored in clear readable text);
- connected Wyndham-branded independently owned hotels to the corporate network without first implementing adequate security measures at those locations;
- failed to fix existing security issues at the branded hotels (putting the entire corporate network at risk);
- allowed servers to use default user IDs and passwords and knowingly letting those servers connect to the corporate network;
- failed to use industry standard password complexity;
- failed to adequately inventory computers connected to its network and was unable to appropriately manage the devices on its network;

- failed to employ reasonable measures to detect and prevent unauthorized access to its computer networks or to conduct security investigations;
- failed to follow incident response procedures; and
- failed to adequately restrict vendors from the main network.[13]

Conclusion

For companies in the United States, the clear affirmation of FTC authority to enforce cybersecurity standards adds to the mounting pressure to build a strong cybersecurity program in the face of increasing security threats and the negative publicity and cost a breach entails. The Wyndham decision also underscores the vulnerability for any company in both judicial rulings and enforcement proceedings of failing to plan and execute an effective response to any breach of confidential consumer information.

—By Tracy E. Miller and Lisa A. Christensen, Bond Schoeneck & King PLLC

Tracy Miller is of counsel in Bond Schoeneck & King's New York, New York, office.

Lisa Christensen is senior counsel in Bond Schoeneck & King's Syracuse, New York, office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] *FTC v. Wyndham Worldwide Corporation*, No. 14-3514 (Third Circuit, Aug. 24, 2015).

[2] 15 U.S.C. § 45(a).

[3] The claim of deception was not before the Third Circuit on appeal.

[4] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises

[5] *Id.* 15 U.S.C. § 45(n), FTC Act Amendments of 1994, Pub.L. No. 103-312, § 9, 108 Stat. 1691, 1695.

[6] Wyndham at 20, citing to Wyndham reply brief at 6.

[7] *Id.* at 21.

[8] FTC guidance is provided informally in draft complaints published together with consent orders that are the result of negotiations with individual companies.

[9] *Wyndham* at 39.

[10] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

[11] Other data security cases can be found at https://www.ftc.gov/enforcement/cases-proceedings#4 and an extensive list of data security resources for businesses can be found at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.

[12] *Wyndham* at 9-10.

[13] Complaint ¶ 24, *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D. N.J. 2014).

Related Articles

- FTC V. Wyndham: How Far Can The FTC Go In Data Security?
- To Business' Chagrin, Cybersecurity Is FTC's Turf Now
- 3rd Circ. Backs FTC In Data Security Row With Wyndham
- FTC Slams Wyndham Bid For Docs On Data Breach Interviews