

Memorandum

In Landmark Decision, Third Circuit Affirms FTC's Power to Regulate Cybersecurity

October 15, 2015

Handing a major victory to the Federal Trade Commission (“FTC”) against the Wyndham hotel chain, the U.S. Court of Appeals for the Third Circuit affirmed the FTC’s long-standing practice of policing companies’ data security practices under the “unfairness” prong of Section 5 of the Federal Trade Commission Act (the “FTC Act”).¹ The decision in *FTC v. Wyndham Worldwide Corp.*² validated a decade of FTC enforcement activity in this sphere, including more than 50 enforcement actions brought against U.S. companies since 2005.³

As the Third Circuit made clear, the FTC does not need to promulgate adjudications or regulations in order to continue this enforcement activity. The court held, however, that the FTC’s published data security guidance and previous complaints served to provide “fair notice” of the FTC’s standards to Wyndham. With FTC Chairwoman Edith Ramirez calling the FTC’s enforcement authority “not only appropriate, but critical,”⁴ U.S. companies should be on fair notice of the FTC’s newly-affirmed authority in the cybersecurity space.

¹ 15 U.S.C. § 45(a).

² *FTC v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015) (hereinafter referred to as “Order”).

³ The *Wyndham* case is the first FTC enforcement action to reach a federal district court. Except for one involving the company LabMD, Inc., all other enforcement actions brought by the FTC have settled, usually accompanied by consent orders.

⁴ Federal Trade Commission, “[Statement from FTC Chairwoman Edith Ramirez on Appellate Ruling in the Wyndham Hotels and Resorts Matter](#),” (August 24, 2015).

“Unfairness” Under the Federal Trade Commission Act

Passed in 1914, the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.”⁵ As the Third Circuit explained, the FTC Act’s language is purposely vague, intended to be a “flexible concept with evolving content.”⁶ Over the past 100 years, the FTC has molded this language to address evolving business practices, including cybersecurity.

The “deception” and “unfairness” prongs of the FTC Act require different tests and analyses. While the FTC has pursued data privacy enforcement actions under the “deception” prong—especially with regard to allegedly deficient or misleading privacy policies—its enforcement activities have largely been driven by the “unfairness” prong. Under Section 5 of the FTC Act, an act or practice is “unfair” if all of the following criteria are met:

1. It causes or is likely to cause substantial injury to consumers;
2. Consumers cannot reasonably avoid such injury; and
3. The injury is not outweighed by countervailing benefits to consumers or competition.

FTC Alleges Unfair Practices in *FTC v. Wyndham*

In 2012, the FTC filed suit against Wyndham in federal district court, alleging that the company’s cybersecurity practices were unfair.⁷ Specifically, the FTC alleged that Wyndham engaged in data security practices that, “taken together, unreasonably and unnecessarily exposed [its] customers’ personal data to unauthorized access and theft.”⁸

A well-known hospitality business, Wyndham licenses its brand to about 90 independently owned hotels, which themselves control the processing of customer information. However, as part of the franchise relationship, Wyndham “manages” these information technology systems and connects them to its own data center in Arizona.⁹

According to the complaint, Wyndham’s systems were hacked on three separate occasions in 2008 and 2009. As a result, the FTC alleged, the credit card information of over 619,000 Wyndham customers was obtained by hackers, resulting in fraudulent charges of at least \$10.6 million. Among other practices, the FTC pointed

⁵ 15 U.S.C. § 45(a).

⁶ Order at 13, citing *FTC v. Bunte Bros.*, 312 U.S. 349, 353 (1941).

⁷ The FTC also alleged that Wyndham’s privacy policy was deceptive, but this issue was not considered in the appeal.

⁸ Am. Compl., *FTC v. Wyndham Worldwide Corp.*, No. 113-1887, ¶ 24 (filed Aug. 9, 2012).

⁹ Order at 7.

to the following alleged failures in cybersecurity:

- Wyndham-branded hotels stored payment card information in clear, readable text;
- Wyndham allowed the use of easily guessable and default passwords to access the property management systems and failed to use firewalls; and
- Wyndham did not employ reasonable measures to detect, monitor and prevent unauthorized access.¹⁰

In response, Wyndham filed a motion to dismiss the case pursuant to Federal Rule of Civil Procedure 12(b)(6), which the district court denied. However, the Third Circuit granted interlocutory appeal on two issues:

1. “whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a) [the FTC Act]”; and
2. “whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision.”¹¹

Third Circuit Affirms the FTC’s Power to Regulate Cybersecurity

In affirming that the FTC holds the authority to regulate cybersecurity, the Third Circuit rejected Wyndham’s argument that recent legislation directing the FTC to enact cybersecurity rules in specific contexts excludes data privacy from the FTC’s reach. According to Wyndham, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act and the Children’s Online Privacy Act require the FTC to establish regulations and standards relating to consumer data in the context of credit reporting agencies, financial institutions and children’s websites, respectively. These “tailored grants” of authority, Wyndham argued, would not be necessary if the FTC already had general authority to regulate cybersecurity.¹² The court rejected this contention, reasoning that the legislation requires the FTC to take specific actions in the cybersecurity realm, sometimes even sidestepping the burdensome procedures usually required when the FTC issues regulations. In sum, the court found that these specific directives did not serve to preclude the FTC’s more expansive authority.

In addition, the court declined to adopt Wyndham’s argument that the FTC itself had made statements in the past that contradicted its present argument for authority. While certain of the FTC’s previous positions acknowledged limits on its authority in certain cybersecurity-related contexts, the court held that these

¹⁰ Am. Compl. at 8-9.

¹¹ Order at 7.

¹² *Id.* at 21-22.

statements were not inconsistent with the FTC's authority to regulate cybersecurity practices generally.

Finally, the Third Circuit rejected Wyndham's contention that a victim of a crime could not be held accountable under the "unfairness" prong of the FTC Act, finding no support for such a statement.

Wyndham Received Fair Notice of the FTC's Cybersecurity Standards

Having found that the FTC has enforcement authority in the cybersecurity realm, the Third Circuit then held that Wyndham received "fair notice" of the FTC's cybersecurity standards because it was only entitled to notice that its conduct could generally "fall within the meaning of" of unfairness under the FTC Act—not notice of the *specific* cybersecurity practices it must follow. Wyndham had argued that it could not know with "ascertainable certainty" what Section 5 required of it in the cybersecurity arena because the FTC had failed to identify exactly what constitutes unfair data privacy practices in FTC rules or adjudications. The court rejected this standard, stating that "the relevant question is not whether Wyndham had fair notice of the *FTC's interpretation* of the statute, but whether Wyndham had fair notice of what the *statute itself* requires."¹³

Moreover, the court wrote, the FTC has "counsel[ed] against" much of Wyndham's alleged misconduct in informal publications and previous complaints.¹⁴ For example, the FTC published a guidebook in 2007 titled "Protecting Personal Information: A Guide for Business,"¹⁵ which includes a checklist of practices that constitute an adequate data security plan. In addition, the FTC filed a number of complaints *before* the Wyndham hacking incidents that address similar allegations. Read together, explained the court, these complaints provided adequate notice of the necessary and sufficient conditions of an alleged violation of Section 5.¹⁶

Conclusion

The Third Circuit's decision in *Wyndham* essentially affirmed the status quo of FTC authority in the cybersecurity arena rather than broadening the agency's powers. It will now be interesting to see whether the FTC will succeed in *proving* unfairness against Wyndham in New Jersey district court. As the first time the FTC filed suit in federal district court for an alleged violation of Section 5 in the cybersecurity context, *Wyndham* is a test case. If the FTC is unable to prove at trial that Wyndham engaged in deceptive and/or unfair business practices—especially if it is unable to prove the requisite substantial consumer harm—other companies may be emboldened to challenge the FTC instead of entering into settlements.

¹³ *Id.* at 35.

¹⁴ *Id.* at 41.

¹⁵ Available at <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

¹⁶ Order at 44-45.

If you have any questions or would like additional information, please do not hesitate to contact any member of the Firm's Privacy and Cybersecurity Practice.

The contents of this publication are for informational purposes only. Neither this publication nor the lawyers who authored it are rendering legal or other professional advice or opinions on specific facts or matters, nor does the distribution of this publication to any person constitute the establishment of an attorney-client relationship. Simpson Thacher & Bartlett LLP assumes no liability in connection with the use of this publication. Please contact your relationship partner if we can be of assistance regarding these important developments. The names and office locations of all of our partners, as well as our recent memoranda, can be obtained from our website, www.simpsonthacher.com.



UNITED STATES

New York
425 Lexington Avenue
New York, NY 10017
+1-212-455-2000

Houston
600 Travis Street, Suite 5400
Houston, TX 77002
+1-713-821-5650

Los Angeles
1999 Avenue of the Stars
Los Angeles, CA 90067
+1-310-407-7500

Palo Alto
2475 Hanover Street
Palo Alto, CA 94304
+1-650-251-5000

Washington, D.C.
900 G Street, NW
Washington, D.C. 20001
+1-202-636-5500

EUROPE

London
CityPoint
One Ropemaker Street
London EC2Y 9HU
England
+44-(0)20-7275-6500

ASIA

Beijing
3901 China World Tower
1 Jian Guo Men Wai Avenue
Beijing 100004
China
+86-10-5965-2999

Hong Kong
ICBC Tower
3 Garden Road, Central
Hong Kong
+852-2514-7600

Seoul
25th Floor, West Tower
Mirae Asset Center 1
26 Eulji-ro 5-Gil, Jung-Gu
Seoul 100-210
Korea
+82-2-6030-3800

Tokyo
Ark Hills Sengokuyama Mori Tower
9-10, Roppongi 1-Chome
Minato-Ku, Tokyo 106-0032
Japan
+81-3-5562-6200

SOUTH AMERICA

São Paulo
Av. Presidente Juscelino
Kubitschek, 1455
São Paulo, SP 04543-011
Brazil
+55-11-3546-1000