THE
NATIONAL LAW REVIEW

FTC v. Wyndham: The Third Circuit Recognizes FTC Authority to Regulate Commercial Cyber Security Practices

SheppardMullin

Article By
Fashion and Apparel Team
Sheppard, Mullin, Richter & Hampton LLP
Fashion & Apparel Law Blog

- Antitrust & Trade Regulation
- Communications, Media & Internet
- Litigation / Trial Practice

- 3rd Circuit (incl. bankruptcy)

Tuesday, September 29, 2015

In 2014, the United States Court of Appeals for the Third Circuit ruling in ***FTC v. Wyndham Worldwide Corporation*** agreed to hear an immediate appeal on two issues: "whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision." On August 24, 2015 the Third Circuit affirmed the decision of the District Court and denied Wyndham's motion to dismiss the complaint.

Factual Background

n 2012, after a two-year investigation into Wyndham's data security practices, the FTC filed suit against the hospitality company alleging that Wyndham had engaged in "unfair … acts or practices" in violation of the Federal Trade Commission Act 15 U.S.C. § 45(a), by failing to take "reasonable and appropriate" measures to adequately secure hotel guests' personal information. Specifically, the FTC alleged that between 2008 and January 2010, hackers gained access on three separate occasions to Wyndham's computer network and that Wyndham engaged in a number of practices that "unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft" including the following:

1. the storage of credit card information in clear, unencrypted text;

2. failure to require employees to use complex user IDs and passwords to access company servers;

3. failure to use readily available security measures, such as firewalls to limit access between the corporate network and the Internet;

4. failure to implement reasonable information security procedures prior to connecting local computer networks to corporate-level networks;

5. failure to "adequately restrict" the access of third-party vendors to its networks;

6. failure to employ reasonable measures to detect and prevent unauthorized access to its computer network or to conduct security investigations; and

7. failure to follow proper incident response procedures.

The FTC's complaint alleged that Wyndham's deficient security practices led and "the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss." Wyndham moved before the United States District Court for the District of New Jersey to dismiss the FTC's complaint arguing that the FTC did not have the authority to regulate bring on unfairness claim involving data security under of §45(a) of the FTC Act. Second, if FTC authorization did in fact exist, the FTC must formerly promulgate regulations before bringing a fairness claim. Wyndham also claimed it did not have fair notice that its specific cybersecurity practices could fall short of that provision. In April 2014, after Wyndham's motion was denied by the District Court, it sought and received an interlocutory appeal from the Third Circuit to settle the matter of authority and notice.

The Third Circuit's Holding: The FTC Had Authority and Wyndham Had Notice

remised largely on the broad authority granted to the FTC under the FTC Act law to protect consumers from unfair and deceptive trade practices, the Third Circuit held that Wyndham failed to show that its alleged conduct "falls outside the plain meaning of 'unfair.'" The Court rejected Wyndham's arguments that extending the FTC's unfairness authority to cybersecurity was tantamount to permitting the FTC to sue grocery stores that are "sloppy about sweeping up banana peels." In response, the Third Circuit observed that were a supermarket to leave "so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability under 45(a)." Accordingly, the Court ruled that the District Court's and FTC's interpretation of Section 45(a) was both consistent with the FTC's prior practice and statutory authority. Furthermore, rejecting Wyndham's request to apply the plain meaning of the word "unfair" to mean "not equitable" or "marked by injustice, partiality, or deception," the Third Circuit reasoned that although unfairness claims usually involve actual harm, the FTC may also bring actions based upon "likely" rather than actual injury. As the Court explained, the FTC Act generally prohibits unfair methods of competition in commerce and, that under the

amendments to the Act, the FTC could deem a practice unfair "if the 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." 15 U.S.C. § 45(n). The Third Circuit noted that when a company "publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of the business" unfairness is present. In relation to the personally identifiable information stolen from Wyndham's computer network, the Court held that consumers could not have reasonably avoided the injury because Wyndham's published privacy policy misled consumers by overstating its cybersecurity practices. The Third Circuit also rejected Wyndham's argument that it was not properly notified of what the FTC expected of Wyndham in terms of "proper" data security. Wyndham argued that the FTC cannot bring an enforcement action without first publishing rules and regulations and did not provide sufficient notice of what the FTC considered reasonable data security methods, thereby denying Wyndham proper due process. The Third Circuit rejected this argument observing that, at this stage of the proceedings, "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." Fair notice, the Court noted, is met if a company could "reasonably foresee that a court could construe [a company's] conduct as falling within the meaning of the statute." Besides, Wyndham was entitled only to a low level of statutory notice here because application of Section 45(a) does not implicate any constitutional rights: (i) the statute is civil not criminal statute; and (ii) statutes regulating economic activity receive a "less strict" test because businesses can be expected to consult relevant legislation in advance of action. Thus, by way of example, Wyndham's lack of "any" firewalls, encryption for certain customer files, weak password requirements, combined with a series of three security breaches, demonstrated that Wyndham knew or should have been on notice of the possibility that a court could find its practices fell short of the fairness requirement of § 45(a). Adding to that calculus, the Third Circuit pointed out that the FTC's 2007 guidebook, *Protecting Personal Information: A Guide for Businesses*, sets forth a checklist of practices that form a "sound data security plan," and noted that other public enforcement actions brought by the FTC should have given Wyndham notice that its repeated alleged failures to protect consumer data could have been considered an unfair practice under the FTC Act.

What Wyndham Means – The Takeaways

In case there were any looming questions as to whether there are legal risks associated with lax cybersecurity, the *Wyndham* decision should provide a definitive affirmative answer. All web-facing companies which collect personally identifiable information are on notice that they routinely must maintain the integrity and security of such consumer data. Companies also must make sure that their privacy policies are accurate and not deceptive. This means ensuring familiarity with and awareness of evolving industry standard security practices and the FTC guidelines derived through the latest security settlements and consent orders posted on the FTC website. If a company does not keep up with industry standards and developments, as recognized by FTC Chairwoman Edith Ramirez, it will be the FTC's responsibility "to hold companies accountable for failing to safeguard consumer

data. It is not only appropriate, but critical, that the FTC has the ability to take action on behalf of consumers when companies fail to take reasonable steps to secure sensitive consumer information." The *Wyndham* decision serves to emphasize a significant problem facing all commercial companies — the protection of the consumer data they collect and hold. Whether one considers that data is intellectual property, private/personal communications, or consumer information, companies need to ensure they are following proper, necessary, and "reasonable" cybersecurity protocols. The challenge, of course, is that "reasonableness" is a moving target driven by technology, hackers, and the industry within which each company operates. As such, it is recommended that companies take cybersecurity precautions that align with industry standards and the NIST Framework and perhaps examine what the federal government is requiring in terms of cybersecurity from its contractors (*see* NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*). While such efforts may never stop cyber -breaches, they should ensure that one avoids scrutiny from the FTC and the potential liability that might result from burying one's head in the sand.