Akin Gump
STRAUSS HAUER & FELD LLP

Cybersecurity, Privacy & Data Protection Alert

August 31, 2015

If you read one thing:

- The Federal Trade Commission (FTC) secured a major appellate victory in its quest to challenge lax corporate cybersecurity practices
- In light of the 3rd Circuit's decision, companies should be on immediate notice that they are likely subject to continued—and, quite possibly, increased—FTC enforcement actions for their cybersecurity practices based on currently existing FTC guidance
- Companies should also become familiar with *Start With Security*, the FTC's recently published (June 2015) cybersecurity guide for businesses that summarizes "lessons learned from FTC cases."

3rd Circuit Affirms FTC's Cybersecurity Oversight

Last week, the Federal Trade Commission (FTC) secured a major appellate victory in its quest to challenge lax corporate cybersecurity practices through its general enforcement authority over "unfair" trade practices. Since 2005, the FTC has brought dozens of administrative actions against companies with allegedly deficient cybersecurity, claiming both "unfair" and "deceptive" practices. Until now, the FTC's complaints had not been the subject of a relevant appellate holding and went largely unchallenged in federal court, with the vast majority—more than 50 cases—resulting in settlement. But, in *FTC v. Wyndham Worldwide Corporation*, the U.S. Court of Appeals for the 3rd Circuit granted the FTC a broad victory in affirming, on interlocutory appeal, the district court's refusal to dismiss an FTC "unfair" trade practices claim against the Wyndham chain of hotels, marking the first time any federal appellate court has given its imprimatur to the FTC's cybersecurity enforcement practices. The 3rd Circuit also rejected Wyndham's fair-notice arguments, finding that Section 5 of the FTC Act gave Wyndham adequate notice of its potential liability such that no additional notice-and-comment rulemaking was required. In light of the 3rd Circuit's broad affirmation of the FTC's cybersecurity enforcement authority without any further requirement of additional rulemaking, companies should be on immediate notice that they are likely subject to continued—and, quite possibly, increased—FTC enforcement actions for their cybersecurity practices based on existing FTC guidance.

Background

On three occasions in 2008 and 2009, hackers allegedly accessed Wyndham's network and obtained payment card information from more than 619,000 customers, which resulted in at least a $10.6 million in loss. Wyndham's privacy policy, which was published on its website, stated that it safeguarded its customers' information using industry standard practices. The FTC sued Wyndham in the U.S. District Court for the District of New Jersey in June 2012 for unfair and deceptive practices in violation of Section

5(a) of the FTC Act based on, among other things, Wyndham's alleged failure to use firewalls, restrict specific IP addresses, encrypt certain customer files, require users to change their default or factory-setting passwords, employ reasonable measures to detect and prevent unauthorized access to its computer network, or follow proper incident response procedures. The district court denied Wyndham's motion to dismiss both the unfair and deceptive practice claims, but certified its decision on the unfairness claim for interlocutory appeal.

FTC's Enforcement Authority over Lax Cybersecurity Practices

Section 5(a) of the FTC Act generally prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a). Wyndham, emphasizing that its business was victimized by criminals, advanced a number of arguments for why its conduct—in essence, according to the FTC, employing lax cybersecurity practices despite its published privacy policy—could not be "unfair" acts or practices within the meaning of Section 5. The 3rd Circuit rejected all of them, holding that Section 5 adequately covered Wyndham's alleged cybersecurity deficiencies.

Wyndham also argued that it lacked proper notice of the FTC's interpretation of what specific cybersecurity practices are required by Section 5(a), but the 3rd Circuit rejected that argument as well. It held that the relevant question was not whether Wyndham had notice of the **FTC's interpretation** of what the FTC Act requires, but rather of what the **Act itself**, as judicially construed, requires. The 3rd Circuit held that Section 5(n) of the Act—which asks whether the challenged "act or practice causes or is likely to cause substantial injury to consumers" and which is not "reasonably avoidable" by consumers and "not outweighed" by countervailing competitive benefits—adequately apprised Wyndham of its potential liability for lax cybersecurity practices. The 3rd Circuit listed several additional considerations causing it to reject Wyndham's fair notice challenge, including a 2007 FTC guidebook, *Protecting Personal Information: A Guide for Business*, which counseled against many of the specific practices in which Wyndham allegedly engaged; a number of FTC complaints and consent decrees in administrative cases raising unfairness claims based on inadequate corporate cybersecurity that were published on the FTC's website; and the alleged weaknesses in Wyndham's own security practices, leading to multiple cyber-attacks, which, in the 3rd Circuit's view, should have made it "painfully clear" that a court could find that its practices would run afoul of the statute.

Implications of the Wyndham Decision

Although the *Wyndham* court was required to accept all the well-pleaded factual allegations in the complaint as true on an interlocutory motion-to-dismiss appeal, it nevertheless stands as a broad affirmation of the FTC's enforcement approach in cybersecurity matters and may further embolden the agency. Companies should expect FTC enforcement that is at least as vigorous as before, and possibly more so. Given the 3rd Circuit's conclusions about fair notice, companies that fail to review and understand public guidance that the FTC has issued or actions it has taken on deficient cybersecurity practices, such as FTC enforcement complaints, consent decrees and publications, do so at their own peril. In this regard, it should be helpful to companies to consider and become familiar with *Start With Security*, the FTC's recently-published cybersecurity guide for businesses that summarizes "lessons

learned from FTC cases."[1] In addition, companies must keep apprised of judicial interpretations of what Section 5(a) requires. Companies should use these materials to examine their own practices to determine whether they are similar enough to any previously condemned actions to be susceptible to FTC enforcement should a breach occur. Of course, the *Wyndham* decision itself serves as an important reference point for companies to use in assessing their cybersecurity practices, particularly with regard to data encryption, controlling network access, readily available security measures and system updates, and detection-and-response systems for data breaches.

Companies should also be aware that some states have their own statutes modeled on the FTC Act. It is possible that unilateral state enforcement against allegedly unfair or deceptive practices related to cybersecurity may increase in the wake of *Wyndham*.

Although other challenges, including the potential for en banc review, may be forthcoming, *Wyndham* marks an important initial victory for the FTC's broad claim to cybersecurity enforcement based on only currently existing guidance, and a decision to which companies nationwide should pay close heed.

[1] Federal Trade Commission, *Start with Security: A Guide For Business* (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

Contact Information

If you have any questions regarding this alert, please contact:

Natasha G. Kohne
nkohne@akingump.com
+971 2.406.8520
Abu Dhabi

Anthony T. Pierce
apierce@akingump.com
+1 202.887.4411
Washington, D.C.

Michelle A. Reed
mreed@akingump.com
+1 214.969.2713
Dallas

David S. Turetsky
dturetsky@akingump.com
+1 202.887.4074
Washington, D.C.

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
+1 202.887.4220
Washington, D.C.

James Edward Tysse
jtysse@akingump.com
+1 202.887.4571
Washington, D.C.

Carolyn C. Mattus
cmattus@akingump.com
+1 212.872.8080
New York