wiley

NEWSLETTER

Wyndham Decision Affirms FTC Jurisdiction and Assertive Role on "Thorny" Cyber and Data Security Issues

April 2014

The Federal Trade Commission (FTC) has just won the first major round of its fight with Wyndham Hotels over data security. In *FTC v. Wyndham Worldwide Corp., et al.,* No. 13-1887 (D.N.J.), the FTC's jurisdiction to punish companies for allegedly lax data security practices was challenged when Wyndham moved to dismiss the FTC's unfair and deceptive practices claims. On April 7, 2014, after briefing, oral argument, and several *amicus* submissions, federal judge Esther Salas rejected all of Wyndham's arguments and affirmed the FTC's jurisdiction. In doing so, she noted that the case highlights "a variety of thorny legal issues that Congress and the courts will continue to grapple with for the foreseeable future." Slip Op. at 6.

The FTC Initiates a High Stakes Legal Battle

Cyber criminals breached the computer networks of Wyndham Hotels & Resorts and Wyndham-branded franchises between 2008 and 2010, stealing customer payment card data. After an investigation, the FTC sued, alleging that Wyndham entities violated Section 5(a) of the FTC Act, prohibiting "unfair or deceptive acts or practices." The FTC alleged Wyndham did not comply with its disseminated privacy policies, and also claimed Wyndham failed to use "reasonable and appropriate" safeguards to protect personal information it collected and maintained, which the FTC claimed was an "unfair" business practice.

Authors

Scott D. Delacourt
Partner
202.719.7459
sdelacourt@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

In April 2013, the Wyndham defendants moved to dismiss both counts, mounting an aggressive attack on FTC authority over general data security. The headline fight centered on the FTC's "unfair" practices claim, which Wyndham attacked as an impermissible expansion of FTC jurisdiction. Wyndham challenged the FTC's power to punish firms for inadequate data security practices under the agency's broad unfairness authority in the absence of clear, binding rules or guidance about what qualifies as "reasonable" data security practices. Wyndham also argued that the FTC's jurisdiction in this area is necessarily limited because Congress has elsewhere provided specific data-security power, and because FTC enforcement would usurp Congress's policy-making role while debate over cybersecurity legislation is ongoing.

The parties also litigated the "deception" claim, disputing, among other things, whether the agency adequately pled consumer injury and whether the FTC must meet heightened pleading requirements under Federal Rule of Civil Procedure 9(b) for deception claims, which Wyndham argued should be treated like fraud allegations.

Judge Salas Affirms the FTC's Approach

Judge Salas rejected all of Wyndham's arguments and denied the motion to dismiss.

The court affirmed the FTC's jurisdiction and its discretion to proceed by enforcement action, rejecting Wyndham's argument that 'the FTC's "'failure to publish any interpretive guidance whatsoever' violates fair notice principles and "bedrock principles of administrative law.'" Slip Op. at 16 (quoting briefing). The court found the unfairness proscriptions in Section 5 to be flexible and noted that the FTC had brought "unfairness actions in a variety of contexts without preexisting rules or regulations." Slip Op. 19. In this sense, the Court found "inapposite" Wyndham's reference to evolving frameworks at the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) as examples of what the FTC should be expected to do. *(See* February 13, 2014 Client Alert). The court analogized the FTC's enforcement action to case-by-case approaches used by the National Labor Relations Board (NLRB) and Occupational Safety and Health Administration (OSHA), despite Wyndham's argument that the "rapidly-evolving nature of data security" made those agencies' actions poor examples. Slip Op. 23.

The court also rejected the challenge to the deceptive practices claim, finding that the FTC had adequately pled it under whatever standard applied.

Going Forward, Expect More Uncertainty, Enforcement, and Litigation

Judge Salas' decision means that the FTC can proceed through discovery; "[a] liability determination is for another day." Slip Op. at 7. Despite her statement that "this decision does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked," Slip Op. at 7, it certainly gives the agency a clear path to bring more cases based on the flexible "reasonableness standard" for unfairness, based on diverse facts.

Wyndham makes clear that many legal battles will have to be fought over the adequacy of private-sector security. The court acknowledged that the future will be rocky, noting that "maintaining privacy is, perhaps, an ongoing struggle," and predicted that "Congress and the courts" will have to deal with "thorny legal issues" for "the foreseeable future." Slip Op. at 6.

These thorny issues will not be limited to critical infrastructure owners, but threaten to ensnare companies of all sizes, many of which do not consider themselves heavily regulated. In the absence of clear guidance about what is reasonable, and with Congress struggling to reach consensus on a legislative solution, companies must pay attention to what the FTC does and what other federal agencies are doing, particularly under the President's Executive Order 13636 on cybersecurity. This includes a Cybersecurity Framework released in February by NIST, which is now informing a variety of agency activities. Unless and until an appeals court disagrees with Judge Salas, companies should expect more case-by-case enforcement actions to be brought by an empowered FTC, and burgeoning demands cropping up throughout the federal regulatory apparatus.

Also see our January 2014 *Bloomberg BNA* article on this case