

FTC Scores Key Victory in Challenge to its Authority to Enforce Data Security

BY [BEHNAM DAYANIM](#) & [MARY-ELIZABETH M. HADLEY](#)

In a much-anticipated decision published April 7, 2014, Judge Esther Salas of the U.S. District Court for the District of New Jersey declined to dismiss the Federal Trade Commission's ("FTC" or "Commission") case against hospitality industry defendant Wyndham Worldwide Corporation. The decision was most significant in its challenge to the Commission's authority to pursue alleged data security issues as "unfair" trade practices. Wyndham argued that the agency's failure first to set out its expectations through the rule-making process was unlawful. That challenge failed, as the court refused to "carve out a data-security exception to the FTC's authority" by requiring "that the FTC publish regulations before filing an unfairness claim in federal court" and found the plaintiff's unfairness and deception claims well-pleaded.¹

Although the court emphasized that it was not making a decision on liability and insisted that the opinion did "not give the FTC a blank check to sustain a lawsuit against every business that has been hacked,"² the opinion provides the Commission an important victory in its ramped-up effort to target data security practices that it deems inadequate.

The Decision

In its motion to dismiss the FTC's complaint, brought under Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), Defendant Wyndham Hotels and Resorts, LLC ("Hotels & Resorts"): (1) challenged the FTC's authority to assert that an alleged deficiency in data security practices could constitute an "unfair" trade practice, (2) argued that the FTC must formally promulgate regulations establishing a data security standard before bringing a claim that particular data security practices are unfair, and (3) contended that the FTC's allegations were insufficiently pleaded to support an unfairness or deception claim.³ Judge Salas rejected all three arguments.

I. The FTC's Unfairness Authority Stands

The court first affirmed the FTC's authority to pursue data security practices as unfair. The court refused to create what it called a data security exception to the FTC's unfairness authority,⁴ and rejected any analogy to *U.S. Food and Drug Administration v. Brown & Williamson Tobacco Corp.*,⁵ in which the Supreme Court held that Congress had not intended to give the FDA the power to regulate tobacco. Rather than agreeing with defendant's assertion that Congress established a "less extensive regulatory scheme" by passing "narrowly-tailored data-security legislation" such as the Gramm-Leach-Bliley ("GLB") Act, the court found that such laws seemed "to complement – not preclude – the FTC's

authority.”⁶ Unlike the FDA’s regulation of tobacco, “the FTC’s unfairness authority over data security can coexist with the existing data-security regulatory scheme.”⁷ Nor was the court convinced that the FTC’s past statements regarding its authority to address data security – including a statement in 2001 that the agency did not have “the jurisdiction to enforce privacy” – evidenced an intent to disclaim that authority.⁸ Judge Salas noted that the FTC’s subsequent actions confirmed its authority in the area and concluded that even if the FTC had altered its position on data security, that alone could not limit its authority.⁹

II. Rules and Regulations Not Required to Satisfy Fair Notice Principles

The court next rejected the argument that fair notice requires the FTC to issue formal rules and regulations before it can file an unfairness claim in federal district court.¹⁰ While recognizing that laws must provide fair notice of forbidden or required conduct, the court was unwilling to conclude that regulations were the only means of doing so.¹¹ Judge Salas explained that Section 5’s proscriptions are flexible¹² and noted that “Circuit Courts of Appeal have affirmed FTC unfairness actions in a variety of contexts *without* preexisting rules or regulations specifically addressing the conduct-at-issue.”¹³ The court found it persuasive that agencies such as the National Labor Relations Board and the Occupational Safety & Health Administration are able to bring enforcement actions without “particularized prohibitions” but rejected as inapposite the fact that the Department of Homeland Security and the National Institute of Standards and Technology “have purportedly managed to craft generalized data-security rules.”¹⁴

III. The Sufficiency of the FTC’s Pleadings in Alleging Substantial, Unavoidable Consumer Harm

Judge Salas’ final findings addressed the sufficiency of the FTC’s pleadings under the FTC Act and Federal Rule of Civil Procedure 8(a). Defendant had argued that the elements of causation and injury had not been met, and that the FTC’s claim of deception required compliance with the heightened pleading standards associated with allegations of fraud pursuant to Federal Rule of Civil Procedure 9(b).

This aspect of the court’s decision is less noteworthy. The court, “drawing inferences in favor of the FTC,” as is required at this stage in the litigation, found that causation and injury had been sufficiently alleged. The court declined to rule on whether the heightened pleading standards of Rule 9(b) apply to claims of deceptive trade practices but found that, in any event, the agency had met its pleading burden.¹⁵

Implications of the Decision

Although the decision is likely to be appealed, the survival of the motion to dismiss is an important initial victory for the FTC. The court’s decision is significant in its treatment of the “unfairness” prong of Section 5 of the FTC Act, establishing the agency’s authority to pursue data security concerns as unfair trade practices even in the absence of regulations establishing substantive security requirements. The rarity of challenges to the FTC’s authority in this area render the decision even more important and likely herald increased agency activity moving forward.



If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

Mary-Elizabeth M. Hadley
1.202.551.1750
maryelizabethhadley@paulhastings.com

San Francisco

Paul M. Schwartz
1.415.856.7090
paulschwartz@paulhastings.com

Thomas P. Brown
1.415.856.7248
tombrown@paulhastings.com

Thomas A. Counts
1.415.856.7077
tomcounts@paulhastings.com

¹ *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-JAD, Dkt. No. 181, at 2, 6 (Apr. 7, 2014). The court indicated that it will address a separate motion to dismiss, Dkt. No. 92, brought by related Wyndham defendants, in a second opinion. *Id.* at 2 n.1.

² *Id.* at 7 (emphasis in original).

³ *Id.* at 2.

⁴ *Id.* at 10.

⁵ 529 U.S. 120 (2000).

⁶ *Id.* at 8, 11 (emphasis in original).

⁷ *Id.* at 12 (citing *Brown & Williamson*, 529 U.S. at 143 (“[I]f tobacco products were within the FDA’s jurisdiction, the Act would require the FDA to remove them from the market entirely. But a ban would contradict Congress’ clear intent as expressed in its more recent, tobacco-specific legislation. The inescapable conclusion is that *there is no room for tobacco products within the FDA’s regulatory scheme.*”) (emphasis added in *Wyndham Worldwide Corp.*).

⁸ *Id.* at 13 (internal citations omitted).

⁹ *Id.* at 13-14.

¹⁰ *Id.* at 18.

¹¹ *Id.* at 21, 22.

¹² *Id.* at 19 (citing *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 385 (1965) (explaining that “[t]his statutory scheme necessarily gives the Commission an influential role in interpreting [Section] 5 and in applying it to the facts of particular cases arising out of unprecedented situations”)).

¹³ *Id.* at 19 (citing *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1153, 1155-59 (9th Cir. 2010) and *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1191, 1193-95 (10th Cir. 2009)) (emphasis in original) (parentheticals omitted).

¹⁴ *Id.* at 22-23 (internal citation and quotation marks omitted).

¹⁵ *Id.* at 38, 42.