wiley

ALERT

Third Circuit Green Lights FTC Data Security Authority, Signaling Companies Must Be Vigilant and Proactive

August 25, 2015

A federal appeals court yesterday resolved a hotly contested case questioning Federal Trade Commission (FTC) authority to police commercial data security practices. The FTC has been aggressive in using its general authority over unfair and deceptive practices to bring more than 50 enforcement actions against companies for apparently inadequate cybersecurity. Reviewing a challenge to the FTC's authority brought by Wyndham Hotels, the U.S. Court of Appeals for the Third Circuit found that the FTC has authority to bring post-hoc enforcement actions against the victims of cyberattacks, where the agency alleges the company used unreasonably lax security measures. The court's opinion sends a clear message to companies that their actions—and inactions—will be scrutinized by regulators and the courts.

This closely-watched test case involved Wyndham Worldwide Corporation—a hospitality company whose systems were hacked three times between 2008 and 2009. The hacks allegedly led to the breach of 600,000 consumer payment card account numbers, causing more than $10.6 million in fraudulent charges. The FTC took action against Wyndham, claiming that its security practices related to its customers' personal data were unfair. Specifically, the FTC alleged that Wyndham's cybersecurity practices were subpar because it:

- allowed hotels to store payment card information in readable text;
- allowed the use of weak passwords;

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Scott D. Delacourt
Partner
202.719.7459
sdelacourt@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Telecom, Media & Technology

- failed to use "readily available security measures," like firewalls or encryption; and
- failed to adequately restrict third-party vendor access to the network.

In response, Wyndham argued that the regulator did not have authority to bring such a claim, because, among other things, the agency had not created clear standards of conduct in advance of the attacks.

Wyndham lost the first round against the FTC in district court, and appealed to the Third Circuit. On appeal, multiple amici weighed in, including the Chamber of Commerce of the United States of America and National Federation of Independent Business for Wyndham, and privacy and consumer groups for the FTC. Ultimately, the Third Circuit found against Wyndham as well.

Writing for the three-judge panel, Judge Ambro flatly rejected all of Wyndham's arguments. The court relied on principles of tort law to reject Wyndham's claim that its conduct fell outside the plain meaning of "unfair," reasoning that the company could be held responsible for foreseeable acts of third parties.

The court also was unpersuaded by the argument that the FTC lacked general data security authority by implication from other, more specific Congressional grants, such as the data security provisions in the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act or the Fair Credit Reporting Act. The court concluded that these specific grants of data security power did not imply that the FTC otherwise lacked general authority.

And the court made quick work of Wyndham's argument that it lacked fair notice of what the FTC saw as reasonable. The court claimed confusion about Wyndham's position on the legal import of prior FTC positions, but ultimately concluded that "Wyndham was not entitled to know with ascertainable certainty the FTC's interpretation of what cybersecurity practices are required by § 45(a). Instead, the relevant question in this appeal is whether Wyndham had fair notice that its conduct could fall within the meaning of the statute." The court noted that difficult notice issues might be relevant if proper resolution of the case turns on deference to the agency's interpretation, but for present purposes, it was enough to find, as the court did, that Wyndham was on notice of Section 5's general unfairness standard.

The court spent some time explaining that Section 5 demands a "cost-benefit analysis" that looks at a "number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity." The court noted that "there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold. But under a due process analysis a company is not entitled to such precision as would eliminate all close calls." The court found the FTC's allegations ample and Wyndham's arguments, which did not claim its practices actually *survive* a reasonable cost benefit analysis, were "too little and too late." The court found Wyndham's arguments weak, "given it was hacked not one or two, but three, times. At least after the second attack, it should have been painfully clear to Wyndham that a court could find its conduct failed the cost-benefit analysis."

This case gives the FTC the green light to continue active involvement in cybersecurity. It also provides a window into the potential reaction of reviewing courts to companies' security decisions. The court pointed out FTC guidance and previous consent decrees, and found that "the FTC's expert views about the characteristics of a 'sound data security plan' could certainly have helped Wyndham determine in advance that its conduct might not survive the cost-benefit analysis."

With the backing of the circuit court, we expect the FTC to double down on its cybersecurity efforts. At oral argument in March, the FTC explained to the court that "if you're a careful general counsel you do pay attention to what the FTC is doing, and you do look at these things." After the Third Circuit's ruling, that statement is particularly apt.