InsideCounsel

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, click the "Reprints" link at the top of any article.

FROM THE SEPTEMBER 2013 ISSUE OF INSIDECOUNSEL MAGAZINE • SUBSCRIBE!

Hotel chain challenges the FTC's power to sue over data breaches

The FTC alleges that Wyndham had "unfair or deceptive" practices by not maintaining "reasonable and appropriate" data security protections

BY MICHAEL KOZUBEK
August 30, 2013 • Reprints

Privacy and data security experts are closely watching a case that for the first time challenges the Federal Trade Commission's (FTC) authority to sue companies on behalf of consumers for cybersecurity breaches and lax or misleading data security policies.

In *Federal Trade Commission v. Wyndham Worldwide Corporation*, the FTC alleges that Wyndham and its hotel subsidiaries violated Section 5 of the FTC Act, which forbids "unfair or deceptive" practices by not maintaining "reasonable and appropriate" data security protections.

The broad authority to protect consumers from data breaches has been the basis of 41 previous investigations of such companies as Google Inc., Twitter Inc. and HTC Corp., resulting in out-of-court settlements and consent decrees. Wyndham is the first company to fight back in court, arguing Congress never granted the FTC cybersecurity oversight and the lawsuit therefore exceeds the FTC's enforcement authority.

"If Wyndham wins, it would disable the ability of the FTC to broadly enforce cybersecurity standards under the guise of consumer protection. I fully expect that the FTC would appeal any such decision to the court of appeals," says Paul Rosenzweig, founder of Red Branch Law & Consulting, which specializes in homeland security and data privacy issues.

Russian Heist

The FTC action grew out of three breaches of the Wyndham data system between June 2008 and January 2010 by a criminal organization based in Russia. The hackers have not been apprehended.

The breaches resulted in the leak of personally identifiable information (PII) from several hundred thousand credit and debit accounts and more than $10 million in fraud losses to consumers, according to the FTC. Wyndham asserts the only PII

taken was credit and debit card information, and there is no proof of actual damage to consumers.

The FTC is asserting its power to regulate deceptive and unfair trade practices under Section 5 in its case against Wyndham. The first claim is that Wyndham made representations to the public that were false and that it could not perform. The second claim is that the defendant engaged in unfair business practices that "caused or [are] likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition."

The FTC seeks a permanent injunction directing Wyndham to better secure its systems, as well as monetary damages.

The FTC filed the case in June 2012, and it subsequently was transferred from the Federal District Court of Arizona to the New Jersey District Court. At press time, a decision on the defendant's motion to dismiss was still pending. The motion contends Congress never granted the FTC broad powers over data security issues.

"Wyndham notes that there are a host of more specific data-security laws already on the books, including the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection Act, Graham-Leach-Bliley and the Fair Credit Reporting Act, suggesting that there has not been a broad, general grant of data-breach security regulatory authority to the FTC," Rosenzweig says.

The defendant's position is supported in an *amicus* brief from a coalition led by the U.S. Chamber of Commerce.

Filling a Void

Some privacy and data security experts see the FTC as filling a void created by the failure of both Congress to pass broad-based privacy legislation and the Obama administration to issue a long-expected executive order setting cybersecurity standards.

"The FTC's efforts are the only aspect of a federal program to compel the business community to adopt more stringent cybersecurity measures," Rosenzweig says. "Cybersecurity legislation is still in the future and the administration's executive order remains in development. The FTC is the only effective game in town."

Because there are no specific federal laws or rules governing consumer cybersecurity, inside counsel seeking to avoid an FTC action must analyze consent decrees issued in previous FTC cases for guidance, says William Baker, of counsel at Wiley Rein.

"The FTC is saying that companies that develop or adhere to strong privacy codes are less likely to be the targets of FTC enforcement actions, even if the companies suffer some breach," Baker says. "Companies that engage in cybersecurity efforts that are based on those that the FTC has sought in consent decrees may feel some degree of practical assurance that they will not be charged by the FTC for failing to maintain reasonable security."

However, what the FTC considers "strong" is still to be determined.

"We are waiting to see whether the FTC will view a code as strong if it does not reflect all of the FTC's own policy preferences," Baker says.

Others say companies need bright-line rules that would come from formal rulemaking.

"Right now, if I am an in-house counsel, I would have to review the various consent decrees and FTC public statements to try to piece together the standards," says Michelle Cohen, an Ifrah Law member. "And doing so would not even cover everything—there would be other practices not yet addressed."

If the FTC went through formal rulemaking proceedings, businesses and other stakeholders would have an opportunity to participate by submitting comments, and at the end of the proceeding would have actual rules to follow, she adds.

EVENTS

© 2013 InsideCounsel. A Summit Business Media publication. All Rights Reserved.