Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FTC V. Wyndham: Recent Developments And Implications

Law360, New York (April 08, 2015, 2:59 PM ET) --

Marc H. Perry

On Friday, March 27, the parties in Federal Trade Commission v. Wyndham — a key data security case with the potential to deeply impact the hospitality industry's cybersecurity practices — filed special supplemental briefs that the Third Circuit Court of Appeals requested during oral arguments earlier in the month. A key question at issue in the case: is the industry on proper notice of the particular cybersecurity standards that the Federal Trade Commission considers sufficient, such that corporations may be subject to FTC sanctions for noncompliance?

- At oral argument, defendant-appellant Wyndham Hotels and Resorts LLC argued strenuously that businesses have essentially no guidance as to what specific cybersecurity practices are required to avoid an enforcement action by the FTC. Wyndham argues that an FTC enforcement action under these circumstances violates constitutional notice principles.

- Plaintiff-appellee FTC argued, just as emphatically, that the business community is in fact on notice of the FTC's cybersecurity requirements by virtue of a variety of complaints that the FTC has filed alleging data privacy failures.

- The court, in detailed questioning during argument, probed whether federal court is the proper forum for the case. Ultimately, the judges requested briefing on whether the matter warrants "detailed administrative consideration," requiring it to be sent instead to an internal FTC proceeding.

Although the case has not yet been decided on the merits — the court is considering Wyndham's motion to dismiss — the potential impact is extreme: this is the first time the FTC has asked a federal court to allow it to interpret its statutory authority to enjoin "unfair" business practices to extend to data security failures.

Wyndham's Alleged Data Breaches and Security Failures

According to the FTC's complaint, Wyndham and the Wyndham-branded hotels to which the Wyndham name is licensed — whose property management systems link to Wyndham's corporate network — suffered three intrusions into their computer networks between April 2008 and January 2010. In each case, hackers were allegedly able to access sensitive consumer data by compromising the Wyndham data center in Phoenix, Arizona. Ultimately, the breaches allegedly led to "fraudulent charges on consumers' accounts, more than $10.6 million in fraud loss, and the export of hundreds of thousands of

consumers' payment card account information to a domain registered in Russia."

The FTC's complaint catalogs the following alleged security failures that purportedly allowed the breaches to occur and which, "taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft:"

- Failure to take appropriate steps — such as employing firewalls — to limit access between and among the Wyndham corporate network, the Wyndham-branded hotels' property management systems, and the Internet;

- Allowing Wyndham-branded hotels to store credit card information in an unencrypted format;

- Not ensuring that Wyndham-branded hotels implemented adequate information security practices before connecting their networks to Wyndham's;

- Not remedying "known security vulnerabilities," including permitting the branded hotels to connect to Wyndham's network with servers whose operating systems could not receive security updates;

- Allowing hotels' servers to connect to Wyndham's network despite the fact that the servers' default user IDs and passwords had never been changed;

- Not doing enough to require strong user IDs and passwords;

- Not adequately inventorying computers connected to Wyndham's network;

- Not taking "reasonable measures" to prevent unauthorized access to Wyndham's network;

- Not following "proper incident response procedures," including failing to monitor Wyndham's network for malware used in a previous intrusion; and

- Not adequately restricting third-party vendors' access to the networks by, e.g., restricting connections to specified IP addresses.

Wyndham's Motion to Dismiss and Appeal

Wyndham moved to dismiss the FTC's complaint in the District of New Jersey, arguing, among other things, that (a) the FTC's statutory authority to take action to enjoin and remedy "unfair" commercial practices does not cover data security failures that are negligent at worst, in which the company itself was a victim of a third party's crime; and (b) the FTC has never put companies on notice of what cybersecurity practices would be sufficient to avoid an enforcement action, raising constitutional concerns.

The district court denied the motion to dismiss, but granted Wyndham's request to allow the denial to be immediately appealed to the Third Circuit. The district court noted pointedly that "the Court does not render a decision on liability today .... And this decision does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked. Instead, the Court denies a motion to dismiss given the allegations in this complaint — which must be taken as true at this stage[.]" In allowing Wyndham to appeal the decision, the court pointed to the "novel, complex statutory interpretation issues" in the case, and acknowledged that those issues "give rise to a substantial ground for difference of opinion."

The Issues Arrive in the Third Circuit

The Third Circuit briefing has been extensive and intense. Eleven days prior to arguments, after some 400 pages of merits briefing (including six friend-of-the-court or amicus briefs), the court issued a letter instructing the parties to come to argument prepared to discuss, in essence, whether the FTC must more fully address the application of its "unfairness" authority to cybersecurity issues via administrative rule-making or internal administrative proceedings, before a federal court can pass on it at all.

The court's question flows from a statutory provision allowing the FTC to seek a permanent injunction only in a "proper case." The meaning of that term is ambiguous, but legislative history could be read to suggest that the provision should only be applied where the FTC "does not desire to further expand upon" its statutory authority, because the case presents no issues "warranting detailed administrative consideration." The court's letter, and the judges at argument, probed whether the question of appropriate cybersecurity practices warrants such administrative consideration.

At oral argument, the FTC responded essentially that (a) the commission has already given the issue its due consideration, both in a recent ruling on a motion to dismiss an administrative proceeding as well as by virtue of filing administrative complaints in "fifty data security cases brought at the administrative level;" and (b) the specific measures that are required to satisfy the FTC's "unfairness" analysis can be established in court on a case-by-case basis as a factual matter, relying on expert testimony and the like. (Wyndham, while emphatically maintaining that the FTC had offered the business community insufficient cybersecurity guidance, opted to "ke[ep its] powder dry" on the question of forum, in large part because "[we] like [our] chances better" in federal court than in an administrative proceeding.)

After oral arguments lasting twice as long as the allotted time, the judges closed the session with a request that the parties brief the forum question.

The Parties' Position on Forum

On March 27, the parties filed the court's requested briefs. Predictably, the FTC's brief reiterated its oral argument position that federal court is an appropriate forum in part because data security complaints and consent decrees filed administratively by the commission constitute whatever "detailed administrative consideration" is required. The FTC's brief also emphasized that Wyndham had never challenged federal courts' ability to hear the case.

In its brief, Wyndham managed to maintain its dry-powder stance. It agreed with the FTC that the court need not, and should not, reach the question of forum because neither party had raised it, arguing that the issue "is not a jurisdictional matter the Court is obligated to address sua sponte."

It went on to argue, among other things, that the case presents a "particularly poor vehicle" to address the issue, in part "because the problems with the FTC's case run far deeper than the form of relief the Commission is seeking or the forum in which it has chosen to proceed." As an example of the issues with the FTC's case, Wyndham cited again its allegation that the industry has never been put on notice of what cybersecurity practices the FTC would accept.

Finally, Wyndham's brief contended that, should the court nonetheless determine to find that federal court is an inappropriate forum for the case, it would be doubly unfair to allow the FTC — after a two-year investigation and nearly three years of federal court litigation — to simply start afresh in its administrative forum. Rather, Wyndham asked the court to dismiss with prejudice, or alternatively to require the FTC to go through a formal rule-making process to set out clearly defined cybersecurity standards to which it will hold the industry.

Potential Implication for the Hospitality Industry

In this case, the FTC has articulated the position that businesses like Wyndham are on notice of required

cybersecurity practices, because the FTC has filed complaints laying out practices which, "taken together," it claims violate the prohibition on "unfair" business practices.

At oral argument, the judges questioned whether businesses could be expected to monitor the FTC's dockets — indeed, it appears that the FTC announced an average of approximately 15 new complaints each month in 2014 — to ensure compliance with its standards. The FTC replied that "any careful general counsel would be looking at what the FTC is doing," because the FTC "has broad-ranging jurisdiction and undertakes frequent actions against all manner of practices and all manner of businesses."

Although the Third Circuit need not follow the district court in accepting that argument, it may. Additionally, the court appears to be considering turning the case away on improper-forum grounds, meaning that a federal court will have no occasion to consider the FTC's position. If that happens, or if the Third Circuit affirms the court below, the FTC will likely continue to maintain that its filing of complaints laying out cybersecurity practices that it considers "unfair" puts businesses and their counsel on notice of the minimum practices they must follow.

In any event, this litigation places the hospitality industry on notice that an investment in uncovering and filling cybersecurity gaps now may prevent FTC sanctions downstream. To this end, monitoring the FTC's complaints and working with information technology staff in making judgments about whether the organization's data security practices sufficiently cover those gaps about which the FTC is complaining is important. This will require attention to detail, an excellent IT staff, and inside and/or outside counsel with a strong working knowledge of cybersecurity principals, both legal and technical.

—By Marc H. Perry and Abraham J. Rein, Post & Schell PC

Marc Perry is a principal in Post & Schell's Philadelphia office and co-chairman of the firm's Hospitality practice.

Abraham Rein is an associate in the firm's Internal Investigations & White Collar Defense practice in Philadelphia.

A version of this article was originally published by HospitalityLawyer on the organization's membership blog, Converge.