The implications of FTC v. Wyndham

November 6, 2015

Although the decision was issued a few months ago, *FTC v. Wyndham* out of the Court of Appeals for the Third Circuit continues to be a hot topic for discussion. The case will likely to have important cybersecurity implications across several industries.

Wyndham, a hospitality company, was subject to three cyber-attacks in 2008 and 2009 that led to hackers obtaining payment card information for 619,000 Wyndham customers. The FTC brought suit, claiming that Wyndham violated 15 U.S.C. § 45(a) of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." Wyndham moved to dismiss, arguing that the FTC did not have authority to regulate cybersecurity under the unfairness prong of § 45(a).

The Third Circuit disagreed, and there are a couple of important takeaways from the opinion. Most notably, businesses should now be aware that, based on *Wyndham*, the FTC indeed has authority to regulate cybersecurity practices. Also according to the Third Circuit: the FTC's authority is pretty broad. Wyndham argued that, even if the FTC has the authority in theory to regulate cybersecurity, the company shouldn't be liable because it didn't have notice of the specific cybersecurity standards required by the unfairness prong of § 45(a). The Third Circuit rejected this argument and instead held that the only notice required was notice that the FTC could regulate cybersecurity in general. (According to the Third Circuit, Wyndham did have or should have had such notice.)

Wyndham is a good reminder that companies should, at minimum, put a basic cybersecurity plan in place and monitor FTC news and guidelines to learn what qualifies as unfair cybersecurity practices according to § 45(a).

Authors