In FTC v. Wyndham Worldwide, Third Circuit Upholds FTC Authority to Enforce Flawed Cybersecurity Measures

By: Robert Van Arnam

08.27.2015

In a much anticipated decision, the Third Circuit Court of Appeals affirmed the authority of the Federal Trade Commission (FTC) to enforce actions against companies who have been subject to a data breach.

The FTC sued global hotel chain Wyndham Worldwide Corporation in 2012 for failing to implement reasonable and appropriate cybersecurity measures in violation of the FTC Act?s prohibition against unfair acts or practices. According to the FTC, Wyndham left customer data unprotected by various security lapses.

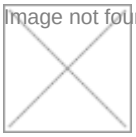
Following an unsuccessful motion to dismiss the unfairness claim, Wyndham appealed to the Third Circuit Court of Appeals on the question of whether a company?s failure to take reasonable cybersecurity measures constitutes an unfair practice under section 5 of the FTC Act in the absence of clear rules on exactly what constitutes reasonable and appropriate cybersecurity practices. The Third Circuit Court of Appeals ruled Tuesday that the FTC could proceed with the lawsuit for Wyndham?s violation of the unfairness and deception prong of Section 5 of the FTC Act by failing to maintain reasonable and appropriate security measures.

The decision is significant for at least three reasons. First, the FTC?s authority to enforce these actions is now upheld and undoubtedly the FTC will flex its powers to take more actions against companies who have a breach. Second, at least for now, no new rules or standards from the FTC are required and companies are on notice of what general actions or inaction violates the Act. In its opinion, the Third Circuit specifically cited an FTC guidebook, 2007 *Protecting Personal Information: A Guide for Business* , which outlined a ?sound data security plan.? It becomes increasingly important for companies to be familiar with FTC guidance on cybersecurity practices as they will help define what is unfair, deceptive or unreasonable to the FTC.

Third, while there is still not one single comprehensive set of rules that businesses can review to ensure

they are in compliance, certain obvious practices will draw the FTC?s attention, including: out of date servers/technology; improper use and maintenance of passwords; insufficient or no encryption; failure to check vendors? websites for alerts about vulnerabilities and for new versions; failure to implement policies including for installing vendor-approved patches and upgrades; and failure to use firewalls and access controls. In the attached chart, the Third Circuit compared the FTC?s allegations against Wyndham and a previous defendant (CSS) finding both sufficiently put the defendants on notice of potential Section 5 violations based on security lapses. *FTC v, Wyndham*, __ F.3d __ (3 rd Cir. August 25, 2015), *45 (citing Complaint, *CardSystems Solutions, Inc.*, No. C-4168 (FTC 2006)).

Data protection will always be a cost-benefits analysis, and no system is entirely secure. However, companies should take these basic measures to avoid becoming the ?low hanging fruit? FTC will likely target next.



Related People

- Robert Van Arnam ? 919.981.4055 ? rvanarnam@williamsmullen.com

Related Services

- Banking & Finance
- Health Care
- Hospitality
- Intellectual Property