Armstrong Teasdale

September 22, 2015 • Advisory • www.atllp.com

WYNDHAM RULING QUESTIONS FTC'S PAST APPROACH TO DATA SECURITY REGULATION

Although the Federal Trade Commission (FTC) was widely hailed as the victor in a recent federal appeals court ruling allowing the FTC's data security breach case to proceed against Wyndham Worldwide Corporation, the decision raises questions about how the FTC has historically regulated information and data security practices.

On August 24, 2015, the Third Circuit Court of Appeals issued an opinion in Federal Trade Commission v. Wyndham Worldwide Corporation, rejecting the defendant's preliminary bid to end the suit accusing it of failing to protect its computers from hackers. Since then, much of the coverage has focused on reports that the Third Circuit acknowledged the authority of the FTC to proceed with a claim that the defendant engaged in unfair practice under Section 5 of the Federal Trade Commission Act (FTCA), which prohibits unfair and deceptive trade practices that cause consumer harm. In particular, the FTC asserted a violation of the FTCA as a result of repeated data theft by hackers.

Perhaps more notable, and as observed by a minority of commentators, such as Justin Hurwitz of Nebraska College of Law on the website www.TechPolicyDaily.com, is what the Wyndham decision says about the FTC's past approach to regulating information and data security practices. Since 2005, the FTC has been pursuing claims against companies with allegedly deficient cybersecurity practices and has resolved many of those claims with consent decrees in administrative cases. The FTC also published a guidebook of practices for a sound data security plan. The FTC has relied on these materials as a type of general law of data security.

The Third Circuit's opinion, however, is critical of the FTC's reliance on this so-called common law. Specifically, the Third Circuit observed that the consent decrees, "were of little use to [Defendant] in trying to understand the specific requirements imposed by [the FTCA]" and that "it may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees." Similarly, the appeals panel observed that "the guidebook could not, on its own, provide 'ascertainable certainty' of the FTC's interpretation of what

PEOPLE

Jeffrey Schultz, CIPP/US

Lucas Amodio, C|EH

F. Scott Galt, CIPP/E

SERVICES AND INDUSTRIES

Litigation

Data Innovation, Security and Privacy

specific cybersecurity practices fail [the FTCA]."

Accordingly, although the Third Circuit's opinion in Wyndham affirms the FTC's authority in the area of information and data security, it calls into question the body of general law regarding information and data security upon which the FTC has historically relied. Furthermore, because the issues addressed by the Third Circuit came up in the context of a motion to dismiss, in which the appeals panel was required to treat all allegations in the complaint as true, the case is far from over and the veracity of the FTC's allegations and the merit of the FTC's theories have yet to be proven. In light of the FTC's ongoing activity in the area of cybersecurity, the Wyndham case is one that members of Armstrong Teasdale's Privacy and Data Security Group will continue to monitor.