New Jersey Federal Court Upholds the FTC’s Authority to Regulate Data Security

JEFFREY L. VAGLE | VAGLEJ@PEPPERLAW.COM
SHARON R. KLEIN | KLEINS@PEPPERLAW.COM

On April 7, a highly anticipated opinion (available at http://thesecuretimes.files.wordpress.com/2014/04/ftc-v-wyndham-opinion.pdf) was issued by New Jersey District Court Judge Esther Salas in a case that will likely have broad implications in the realms of privacy and data security. The case in question is FTC v. Wyndham Worldwide Corp. et al., where the defendant has raised fundamental challenges to the Federal Trade Commission (FTC)'s power to regulate data security under the FTC Act. Through a motion to dismiss, Wyndham argued that the FTC had no authority to assert a claim in the data security context, that the FTC must first formally promulgate data security regulations before bringing such a claim, and that the FTC's pleadings of consumer harm were insufficient to support their claims. The Wyndham court sided with the FTC on all of these arguments, and dismissed Wyndham's motion to dismiss.

In order to better grasp the context and implications of this decisions, some background is in order. On June 26, 2012, the FTC filed a complaint in Arizona Federal District Court against Wyndham Worldwide Corporation, alleging that Wyndham "fail[ed] to maintain reasonable security" on their computer networks, which led to a data breach resulting in the theft of payment card data for hundreds of thousands of Wyndham customers, and more than $10.6 million in fraudulent charges on customers' accounts. Specifically, the complaint alleged that Wyndham engaged in deceptive business practices in violation of Section 5 of the FTC Act by misrepresenting the security measures it undertook to protect customers' personal information. The complaint also alleged that Wyndham's failure to provide reasonable data security is an unfair trade practice, also in violation of Section 5.

On August 27, 2012, Wyndham responded by filing a motion to dismiss the FTC's complaint, asserting, *inter alia*, that the FTC lacked the statutory authority to "establish data-security standards for the private sector and enforce those standards in federal court," thus challenging the FTC's authority to bring the unfairness count under the FTC Act. The case was transferred to the Federal District of New Jersey on March 25, 2013, and Wyndham's motions to dismiss were denied. On April 26, 2013, Wyndham once again filed motions to dismiss the FTC’s complaint, again asserting that the FTC lacked the legal authority to legislate data security standards for private businesses under Section 5 of the FTC Act.

At stake in this litigation is the FTC’s ability to bring enforcement claims against companies that suffer data breach due to a lack of “reasonable security.” The FTC has taken the lead on data security regulation for well over a decade, claiming that poor data security is a violation of the FTC Act, which prohibits “unfair or deceptive acts or practices in or affecting commerce.” If the court granted Wyndham's motion on these grounds, much of that regulatory history would be called into question.

In her April 7 opinion, Judge Salas turned first to Wyndham's assertion that the FTC lacks the statutory authority to regulate data security practices for every American company. Wyndham pointed out that Congress has limited the FTC's data security power to only certain, well-defined areas, citing the Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), and the Children's Online Privacy Protection Act (COPPA) as evidence of these boundaries. Judge Salas rejected this argument, holding that "subsequent data-security legislation seems to complement—not preclude—the FTC's authority."
The court next addressed Wyndham's argument that, even if the FTC is correct in its understanding of the statutes, they have not provided businesses fair notice required by the Due Process Clause. Wyndham pointed out that the “FTC has not published any rules, regulations, or guidelines explaining to businesses what data-security protections they must employ to comply with the FTC’s interpretation of Section 5 of the FTC Act.” This has been a growing concern among U.S. businesses, which face a daily struggle against data breaches and other related information security incidents, and are unsure of what “reasonable data security practices” might mean. Judge Salas held, however, that the FTC’s interpretations of the FTC Act “while not controlling upon the courts by reason of their authority, do constitute a body of experience and informed judgment to which courts and litigants may properly resort for guidance.”

Finally, with respect to Wyndham’s claim that the FTC failed to sufficiently plead harm to consumers, the court observed that the FTC’s claims were that “data-security practices caused theft of personal data, which ultimately caused substantial injury to consumers.” As Judge Salas was quick to point out, the court did not render any decision with respect to liability in this opinion, which only addressed the motion to dismiss before it. The court also stated that “this decision does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked.” (emphasis in original). But the fact remains that the FTC has prevailed here on a fundamental point. While it is difficult to tell at this point how this case will progress, the FTC can, at the very least, continue with its current data privacy regulation regime, and might take this decision as a cue to expand its role in this area. We advise companies to take the time to review FTC reports, complaints, and consent decrees (available at http://business.ftc.gov/privacy-and-security/data-security) to ensure that they are steering clear of the specific data security practices the FTC has cited as flawed or insufficient. Pepper’s Privacy, Security, and Data Protection Practice Group has the knowledge and experience to provide actionable assistance in this rapidly changing field.

RSS on www.pepperlaw.com

Subscribe to the latest Pepper articles via RSS feeds. Visit www.pepperlaw.com today and click on the RSS button on the publications page to subscribe to our latest articles in your news reader.