CRS Reports & Analysis

Legal Sidebar

Third Circuit Affirms the FTC's Authority to Regulate Data Security as an Unfair Trade Practice

09/21/2015

On August 24, the U.S. Court of Appeals for the Third Circuit (Third Circuit) in *FTC v. Wyndham Worldwide Corp*. issued an opinion affirming the decision of the U.S. District Court for the District of New Jersey that the Federal Trade Commission (FTC) has authority to regulate companies' data security practices under the unfairness prong of Section 5 of the Federal Trade Commission Act (Section 5), which was discussed in an earlier Legal Sidebar. The case was returned to the district court for further proceedings that could address the merits of whether global hospitality company Wyndham Worldwide Corp.'s (Wyndham) cybersecurity policies were inadequate.

The FTC originally filed its lawsuit in 2012 against the hotel chain and three of its subsidiaries, after several data breaches occurred involving the personal information of its customers. The agency argued that Wyndham's privacy policy misrepresented the security of customer information and that its failure to safeguard personal information caused substantial consumer injury. Specifically, the FTC alleged that wrongly configured software, weak passwords, and insecure computer servers led to three data breaches at Wyndham hotels from 2008 to 2009, compromising more than 619,000 payment card accounts and transferring customers' payment card account numbers to locations in Russia. The FTC alleged that the computer intrusions led to more than $10.6 million in fraud losses.

Based on those allegations, the agency claimed that Wyndham engaged in unfair cybersecurity practices that unreasonably and unnecessarily exposed consumers' personal information to unauthorized access and theft, and that Wyndham's security practices were "unfair and deceptive" in violation of Section 5 of the FTC Act. Wyndham contested the allegations and argued, among other things, that the FTC had exceeded its statutory authority to assert an unfairness claim in the data security context, and that the agency failed to provide the company with fair notice of the specific cybersecurity standards the company was required to follow.

On April 7, 2014, a federal district court judge in New Jersey, denied Wyndham's motion to dismiss the case, rejecting Wyndham's position that the FTC lacked statutory authority to regulate data security. Although the opinion did not address the merits of whether Wyndham's security policies were inadequate, the judge did undertake, in a 42-page opinion, an in-depth analysis of the FTC's authority. For more on the district court's opinion, see this CRS Report.

The Third Circuit examined the legislative history of the unfairness prong and found that Congress chose not to list specific unfair practices, but rather designed the term as a "flexible concept with evolving content" and "intentionally left its development to the Commission." The Third Circuit then reviewed agency adjudications and policy statements on unfairness, judicial opinions, and statutory amendments related to unfairness. The court concluded that the test for unfairness was 1) whether the conduct caused substantial injury to consumers; 2) the injury was not reasonably avoidable by consumers; and 3) the injury was not outweighed by countervailing benefits to consumers or competition. The Third Circuit found that the FTC's allegations about Wyndham's cybersecurity practices met the criteria for unfairness under Section 5.

The Third Circuit dismissed Wyndham's argument that Congress excluded cybersecurity from the FTC's unfairness authority by enacting other laws requiring the FTC to regulate cybersecurity in specific contexts (The Fair Credit Reporting Act's Disposal Rule for Consumer Data, the FTC's Safeguards Rule required by the Gramm-Leach-Bliley

Act, and the Children's Online Privacy Protection Act Rule). The Third Circuit distinguished *FDA v. Brown & Williamson Tobacco Corp.*, concluding that there the inference of Congress's intent to exclude tobacco-related products from the FDA's authority by enacting subsequent statutes regulating tobacco was far stronger. The court also disagreed with Wyndham's position that Congress would not have enacted several other statutes that impose obligations upon businesses to protect consumer data if the FTC already had authority over cybersecurity, because each of those laws specifically require the FTC to issue regulations as opposed to giving the FTC broad authority.

The court dismissed Wyndham's argument that the agency's past statements contradicted its assertion of authority to regulate cybersecurity practices. The court noted that the agency had remarked that some cybersecurity practices are unfair, and that in its two previous statements the FTC only acknowledged that it could not require companies to adopt fair information practice policies. Ultimately, it concluded that the FTC's unfair cybersecurity actions are not inconsistent with the agency's earlier positions.

The Third Circuit also addressed Wyndham's due process claim—that it lacked notice from the FTC of what cybersecurity standards were required. The court concluded that Wyndham had adequate notice of what cybersecurity measures could be required under the statute based on a cost-benefit analysis derived from Section 5(n) "that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity"; an FTC Guidebook for Businesses which provides a checklist of security practices to create a sound data security plan; and four to five FTC administrative cases alleging inadequate data security practices filed before Wyndham's data breach.

The *Wyndham* decision is the first court of appeals decision to address the FTC's authority under the unfairness prong of Section 5 to regulate lax data security practices that may lead to data breaches. Since 2002, the FTC has pursued more than 50 investigations of such practices under Section 5, which prohibits unfair or deceptive acts or practices in commerce. Because most of the FTC's privacy and data security cases were settled or abandoned, there have been few judicial decisions on the scope of the agency's authority in the cybersecurity context. FTC data security settlements typically require violators to maintain a comprehensive information security program, to obtain bi-annual audits from an independent third-party security professional for twenty years, and to provide consumer redress. The decision permits the FTC to continue to pursue companies whose computer systems suffer a data breach and fail to protect consumers' data. It is widely believed that the FTC will step-up its enforcement efforts against companies with data security practices that have caused substantial injury to consumers. Others hope that Congress will elaborate on what specific cybersecurity standards companies should be required to follow.

As part of efforts to enact cyber and data security legislation, several bills before Congress include provisions that would provide the FTC with enhanced enforcement authority by, for example, authorizing the FTC to issue rules to implement data security standards and to assess civil penalties. In recent testimony before Congress, the agency has called for federal legislation that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies to provide notification to consumers where there is a data security breach. In both of those areas, the FTC seeks the ability to impose civil penalties and the authority to issue administrative rules.