August 27, 2015

This week, the Third Circuit issued its much-awaited decision in *FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. Aug. 24, 2015). The Court unanimously affirmed the FTC's authority to bring actions challenging businesses' data security practices under the "unfairness prong" of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a), without first promulgating rules or regulations that describe acceptable data security standards.

The FTC's enforcement action against Wyndham

From 2008-09, Wyndham experienced three data breaches in which more than 619,000 payment cards were allegedly compromised, resulting in $10.6 million in fraudulent charges. In 2012, the FTC filed a federal enforcement action against Wyndham, alleging in pertinent part that Wyndham's data security practices unreasonably and unnecessarily exposed consumers' personal data to hackers in violation of Section 5's unfairness prong, which prohibits "unfair … acts or practices in or affecting commerce." Wyndham allegedly failed to use "readily available" security measures such as firewalls and encryption, allowed the use of easily-guessed passwords to access its network, and otherwise did not use "reasonable measures" to prevent and detect data breaches.

In the past decade, the FTC has commenced dozens of enforcement actions similar to the Wyndham case, asserting that it has authority to challenge companies' data security practices under Section 5. Most actions have led to settlements in which the companies have agreed to implement comprehensive data security plans and consented to 20 years of outside monitoring. In contrast, Wyndham moved to dismiss, contending that the FTC's traditional consumer protection authority under Section 5 did not apply to data security. The district court denied Wyndham's motion to dismiss, and the Third Circuit granted interlocutory review of two issues: (1) whether Section 5's unfairness prong authorizes the FTC to regulate companies' data security practices; and (2) if so, whether Wyndham received fair notice that its data security practices might fall short of Section 5's requirements.

The Third Circuit's decision

The court unanimously rejected each of Wyndham's arguments.

First, Wyndham argued that Section 5's unfairness prong does not cover data security, citing recent statutes (e.g., the Fair Credit Reporting Act and the Children's Online Privacy Protection Act) that granted the FTC tailored authority to regulate data security in distinct sectors. Wyndham contended that these tailored grants would have been unnecessary if the FTC already had plenary authority to police data security under Section 5. The Court rejected Wyndham's argument, holding that the recent statutes granted the FTC new data security powers that complemented its existing Section 5 authority over data security.

Second, Wyndham contended that even if the FTC had authority to regulate data security under Section 5's unfairness prong, its enforcement action violated due process. Wyndham argued that because the FTC has not issued regulations describing minimum required data security practices, Wyndham lacked "fair notice" of its Section 5 data security obligations. However, the Court held that Wyndham was not entitled to notice of specific data security practices that the FTC viewed as satisfactory. Rather, due process entitled Wyndham only to fair notice that a court could find its alleged data security practices inadequate under Section 5—and Wyndham had received such notice.

Specifically, the Court held that while Section 5 is "far from precise," in 1994 Congress codified the FTC's 1980 Unfairness Policy which requires the FTC to find substantial injury to consumers which is not reasonably avoided by such consumers and is not outweighed by countervailing benefits to consumers before declaring conduct to be unfair. That it places companies on notice that they must conduct a cost-benefit analysis that weighs "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." Here, because Wyndham experienced three data breaches, it was on notice after the second breach that a court could find its data security practices deficient under Section 5's cost-benefit analysis. Moreover, the FTC had issued informal guidance and complaints and consent decrees in other cases; these illustrated that the FTC had indicated that specific data security practices used by Wyndham were defective. The FTC had even filed nearly analogous allegations against a different company in a 2006 enforcement action.

Wyndham also argued that its alleged conduct did not satisfy the plain meaning of an "unfair" act, as it was the victim of a data breach that had not acted unscrupulously or unethically towards its customers. But the Court held that the FTC could pursue an action under Section 5's unfairness prong against a company whose allegedly deficient security practices led to a data breach in which consumers were actually harmed. (The Court also observed in dicta that while unfairness claims "usually involve actual and completed harms," the FTC could also bring unfairness claims "on the basis of likely rather than actual injury.")

Practical considerations

The decision is a victory for the FTC, which has long asserted that Section 5 general language allows it to bring enforcement actions against companies whose deficient data security practices have resulted in data breaches. The FTC may also invoke the Third Circuit's dicta to bring enforcement actions against companies whose data security practices (in the FTC's view) will *likely* cause consumers harm, even if no consumers have suffered actual injury.

It remains to be seen whether the FTC will increase its data security enforcement efforts with the Third Circuit's decision now in its pocket. Nonetheless, to reduce the risk of an FTC enforcement action, companies should consider evaluating the adequacy of their data security practices in light of the FTC's prior guidance and prior Section 5 complaints and settlements.

Key Contacts

Matthew D. Brown San Francisco	brownmd@cooley.com +1 415 693 2188

Howard Morse Washington, DC	hmorse@cooley.com +1 202 842 7852
Bethany Lobo San Francisco	blobo@cooley.com +1 415 693 2187
Scott Dailard San Diego	sdailard@cooley.com +1 858 550 6062
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090