Crowell

# CLIENT ALERT

## Third Circuit Upholds the FTC's Authority to Regulate 'Unfair' Data Security Practices

**August 26, 2015**

On Monday, the Third Circuit issued its much-awaited decision in *FTC v. Wyndham Worldwide et al.* and held that the Federal Trade Commission (FTC) has statutory authority under Section 5 of the FTC Act to bring enforcement actions against defendants for allegedly "unfair" data security practices.

**Case Background**

The road to the Third Circuit's decision began in 2008, when Wyndham suffered the first of three cyberattacks that exposed customer financial information and resulted in unauthorized charges to customers. The FTC sued Wyndham in 2012 for both deceptive and unfair practices under Section 5 of the FTC Act. In particular, the FTC claimed that Wyndham failed to implement sufficient network and data safeguards, including those related to firewalls, encryption, and user IDs and passwords. Wyndham moved to dismiss the complaint on the grounds that the FTC lacked authority to regulate data security practices under its unfairness authority and failed to provide fair notice of the applicable cybersecurity standards. Among other arguments, Wyndham asserted that the FTC's exercise of general cybersecurity authority under the FTC Act was inconsistent with later, more specific grants of FTC cybersecurity authority in the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and Children's Online Privacy Protection Act (COPPA), and also with the FTC's repeated assertions of its limited cybersecurity enforcement powers and its requests for additional cybersecurity authority.

In 2014, the New Jersey district court denied Wyndham's motion to dismiss and held that more specific statutes and requests for expanded authority complemented rather than preempted existing FTC authority and also that the FTC need not promulgate specific rules for data security before attempting to enforce them on a case-by-case basis. It did, however, certify the issue for interlocutory appeal to the Third Circuit.

**The Third Circuit's Decision**

Despite apparent skepticism during oral arguments, the Third Circuit Panel agreed with the lower court and unanimously upheld the FTC's statutory authority over unfair cybersecurity practices. The Panel also concluded that Congress deliberately left undefined the unfair practices that the FTC is empowered to pursue under the FTC Act. The language underlying the FTC's authority is thus a "flexible concept with evolving content." With regard to cybersecurity, the Panel concluded that the relevant legal issue was whether Wyndham "had fair notice that its conduct could fall within the meaning" of the FTC Act, not whether it had notice of the specific security practices that the FTC would deem unreasonable. The Panel further noted that the FTC previously pursued unfairness actions based on inadequate data security practices, and had also previously published guidance in which it identified proper data security measures.

**What the Decision Means**

Although the Third Circuit's decision is potentially subject to a motion for reconsideration or further appeal, and the underlying case remains pending in district court, the FTC will likely view the Third Circuit's decision as a vindication of its privacy and data security enforcement and policy activities to date. The FTC is pursuing a similar administrative action against LabMD, which has had its own ups and downs before the FTC administrative law judge, Congress, and federal courts. The FTC may choose to rely on the Third Circuit's decision to push that case to settlement rather than continue to seek victory on the merits.

The Third Circuit's decision comes at a time when the FTC's role as the nation's "privacy regulator" has never been stronger. And earlier this year, the Obama Administration proposed legislation that would allow the FTC to enforce a "Consumer Privacy Bill of Rights" against a wide array of entities, including non-profits, as well as to approve industry codes of conduct to protect personal information.

The FTC will continue to play an aggressive role in identifying and eliminating—through policy, education, and enforcement activities—what it deems to be unreasonable data security practices. Companies across all industries regulated by the FTC should thus actively and periodically review and, as needed, revise their data security policies and practices in accordance with FTC guidance. In addition, given the Third Circuit's linkage of privacy policies with data security practices, companies should review their privacy statements to ensure an accurate reflection of their current data security practices.

---

**Other Articles in This Month's Edition:**



---

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.


**Jeffrey L. Poston**
Partner – Washington, D.C.
Phone: +1.202.624.2775
Email: jposton@crowell.com

**Christopher A. Cole**
Partner – Washington, D.C.
Phone: +1.202.624.2701

Email: ccole@crowell.com

**Kate M. Growley, CIPP/G, CIPP/US**
Partner – Washington, D.C.
Phone: +1.202.624.2698
Email: kgrowley@crowell.com