Another Cybersecurity Wake-up Call for Business

By Jennifer Woods / Sep 21, 2015

On August 24, 2015, the U.S. Court of Appeals for the Third Circuit released its long-awaited ruling in *Federal Trade Commission v. Wyndham Hotels*, affirming the FTC's enforcement powers in the cybersecurity sphere. The decision is important because it ratifies the FTC's current enforcement strategies in policing security practices which the FTC determines are "unfair" to consumers. After Wyndham's network and the property management systems of Wyndham-branded hotels suffered three separate data breaches in 2008 and 2009, the Federal Trade Commission ("FTC") initiated suit alleging that Wyndham engaged in "unfair" and "deceptive" acts and practices within the meaning of Section 5 of the FTC Act. Specifically, the FTC alleged that Wyndham unfairly failed to use reasonable security measures by storing payment card information in plain text, using weak passwords, failing to use firewalls, failing to maintain records of computer network connections, failure to require branded hotels to use up-to-date software, failure to adequately restrict third-party access to its networks, failure to employ reasonable measures to detect and prevent unauthorized access and investigate security breaches, and failure to implement proper incident response and remediation procedures.

Wyndham moved to dismiss the FTC's complaint for failure to state a claim under Fed. R. Civ. P. 12(b)(6) on the grounds that (1) the FTC does not have authority to regulate cybersecurity as unfair practices and (2) the FTC had not taken sufficient steps to provide businesses with fair notice of the FTC's interpretation as to which cybersecurity practices are unfair. The district court denied the motion. The Third Circuit agreed to hear Wyndham's appeal as to the denial of dismissal of the "unfairness" claim.

The Third Circuit's opinion affirmed the district court's ruling in all respects. The court found that the complained-of conduct fell within the plain meaning of "unfair," and that FTC has the authority to regulate cybersecurity practices through adjudication and without formal rulemaking. The court found that Wyndham had fair notice of what was required under the FTC Act, but was not entitled to know with ascertainable certainty the FTC's interpretation of the statute. The relevant inquiry consists of a cost-benefit analysis that takes into account a number of factors, including the "probability and expected size of reasonably unavoidable harms to consumers" associated with the various levels of cybersecurity and the relative costs to businesses and consumers at each of the various levels, as well as the costs to the business and consumers resulting from an investment in better cybersecurity.

The Third Circuit also noted that the circumstances surrounding the FTC's complaint underscored its finding that Wyndham had fair notice that its conduct might fail the cost-benefit analysis. The court noted that Wyndham was hacked "not one or two, but three, times," which should have made it "painfully clear" to Wyndham that its conduct failed the cost-benefit test and was potentially actionable. The FTC publishes complaints, consent decrees, and business guidance, including its 2007 guidebook entitled Protecting Personal Information: A Guide for Business which assist businesses in determining which conduct is likely to invite an FTC investigation.

While the appeal was pending, the FTC has recently published another guidebook, Start with Security: A Guide for Business that includes "lessons learned" from FTC cybersecurity enforcement cases.

The *Wyndham* case is significant in that it ratifies the FTC's current approach to enforcing its mandate under Section 5 in the context of cybersecurity. What this means is that the FTC expects businesses to conduct risk analyses of their cybersecurity practices and consider the potential impact of those practices on consumers. Failing to conduct such a cost-benefit analysis (risk assessment) and adopt reasonable cybersecurity practices in light of the results may result in FTC scrutiny. Companies should pay close attention to FTC pronouncements in this area, including consent decrees, blog posts, and published business guidance, for assistance in determining which cybersecurity practices have been determined by the FTC to fail the cost-benefit analysis. Companies should also take note of the practices described in the *Wyndham* complaint and, particularly where the company has already experienced a security breach, take note of any security improvements which may be required or recommended to protect consumer information from similar breaches in the future.

If you have any questions regarding this alert, please contact Jennifer Woods at (312) 985-5931 or jwoods@clarkhill.com, or any member of the Clark Hill Cybersecurity, Data Protection & Privacy Group.

 |