FTC v. Wyndham Worldwide Group – A Warning From the 3rd Circuit

Insights
9.18.15

On August 24, in *FTC v. Wyndham Worldwide Corp. et al*, the 3rd Circuit Court of Appeals affirmed that the FTC could enforce its own **reasonable interpretation** of what cybersecurity standards are necessary to avoid prosecution from the FTC for unfair methods of competition.Reading between the lines, the decision allows the FTC to heighten its enforcement standards without any change in regulations.The ruling is not surprising, given that the court also found some of Wyndham's representations regarding cybersecurity measures were fraudulent.On its face, the decision imposes greater requirements on companies who retain sensitive information about customers and employees, however it also provides guidance, where there once was little, about what types of practices are important or necessary.

The court found that over the course of several years, the following practices, in conjunction, were unacceptable:

- The company failed to implement updates to its operating systems over three years.
- The company permitted access through "critical network points" using default or factory-setting passwords.
- The company did not restrict access to sensitive information using a firewall or equivalent security measure.
- The company did not adequately train its employees to implement information security policies.
- The company did not adequately restrict access of third-party vendors to its network and servers.
- The company failed to identify the source of at least one of the cybersecurity attacks and recognize repeated patterns of security breach.
- The company did not adequately investigate thee breaches of its systems that it did discover.

The comfort is that the list must be read in conjunction—in the present, the FTC would be hard-pressed to find a company that is remotely concerned with its cybersecurity following the same pattern of behavior found in the *Wyndham* case.

The difficult requirement to augur is whether your company can quickly and adequately respond to a cybersecurity attack and what that means one year from today.After all, was it possible seven years

cybersecurity attack and what that means one year from today. After all, was it possible seven years ago before "data-centric security" was common security parlance?