Third Circuit Affirms FTC Authority to Regulate Cybersecurity

by Batya F. Forsyth & William T. Kellermann

If it wasn't clear before, data breaches are now a federal affair, in addition to falling under various statutes and regulations in 47 states. Since 2000, the Federal Trade Commission (FTC) is the self-styled "primary federal data security regulator" in the United States. Beginning in 2005, the FTC instituted numerous data security enforcement actions, primarily under authority found in Section 5 of the Federal Trade Commission Act. Yet nowhere in the Act are there explicit references to "data privacy," "data security" or the more modern moniker, "cybersecurity."

Until recently, targets of FTC investigations or enforcement actions arising from data breaches have chosen administrative settlements rather than fight. That changed as a result of the Wyndham Worldwide hotel chain data breaches and Wyndham's subsequent resistance to FTC enforcement. Under the recent ruling in *Federal Trade Commission v. Wyndham Worldwide Corporation, et al.*, __ F.3d __, 2015 WL 4998121 (3d Cir. Aug. 24, 2015), FTC regulatory authority appears to be on solid ground.

Section 5 of the FTC Act grants the FTC broad authority to prevent the use of unfair and deceptive trade practices. 15 U.S.C. § 45(a)(1) and (2). While banks, savings and loans, federal credit unions and transportation companies are exempt, 15 U.S.C. § 45 (a)(2), the Act otherwise casts a broad net across industries.

Wyndham Worldwide owns or operates a hotel chain and provides centralized IT services to franchises, as well as its own properties. The FTC enforcement action stemmed from a series of data breaches that gave hackers access to payment card information for more than 619,000 customers. The hacks later gave rise to more than $10.6 million in fraudulent charges.

The FTC brought its action against Wyndham in the United States District Court for the District of New Jersey alleging the company's data security practices were an "unfair practice" and that its privacy policy was "deceptive" under Section 5 of the Act. The FTC complaint alleged Wyndham misrepresented the security measures it took to protect customers' personal information, and that Wyndham’s cybersecurity efforts were unfair in the face of the FTC’s published security guidance. The District Court denied Wyndham's motion to dismiss, finding the FTC had

the authority to regulate data security practices. Notably, the Court further found the FTC did not have to issue formal regulations before bringing enforcement actions. The Third Circuit certified two issues for interlocutory appeal:

1. Whether the FTC has authority to regulate cybersecurity under the unfairness prong of 15 U.S.C. § 45 (a); and,
2. Assuming such regulatory authority, whether Wyndham had fair notice that its specific cybersecurity practices could fall short of the statutory requirement.

The Third Circuit affirmed the District Court finding ample authority for the FTC to regulate cybersecurity under the Act, as well as clear guidance under the Act, the FTC's regulatory enforcement history and published guidance as to acceptable conduct in setting cybersecurity policies and practices.

While the FTC Act grants the FTC both rulemaking and enforcement authority under Section 5, the FTC has not enacted formal rules or regulations that apply to data security requirements. As set forth in the *Wyndham Worldwide* order, companies must rely on FTC publications, data security complaints and consent decrees to determine if their data security programs comply with FTC standards. To that end, the FTC published *Protecting Personal Information, A Guide for Business* which sets forth five principles on which a company must base its data security practices:

- Be aware of all the personal information collected, retained and shared.
- Keep only personal information required for legitimate business operations.
- Use physical and electronic security to protect the information an organization retains.
- Properly dispose of personal information as soon as it is no longer necessary for business operations.
- Have a plan to respond to security incidents.

The FTC is seen as having a central role in protecting consumers. However, just as the FTC Act is silent on the topic of data security, nothing in 15 U.S.C. § 45(a) limits the FTC's authority to "consumer" data *per se*. The Act empowers the Commission to address "unfair or deceptive acts or practices in or affecting commerce." That broad mandate, coupled with the guidelines established by the Commission and the holding in the *Wyndham* opinion strongly suggests all companies must now address their cybersecurity policies and practices. Companies must ensure the policies and practices meet the guidelines set by the FTC, at least with respect to the personally identifiable information (PII) of employees, contractors and business partners that finds its way onto company systems.

The first four bullets of the FTC Guidelines are essential elements of an Information Governance (IG) program. One could argue after the *Wyndham* opinion that the failure to institute an information governance program puts an enterprise squarely in the sights of a costly and time consuming FTC enforcement action in the event of a data breach. Conversely, implementing an IG program, coupled with a well-crafted cyber incident response plan, will help a company stave off or mitigate the effects of FTC scrutiny. Moreover, an IG program comes with added benefits of reduced cost and risk associated with data storage as well as reduced cost whenever a company must respond for compliance or other investigations or to parties in litigation. If your company has not considered an IG program before now, perhaps now is the time.

.....

Hanson Bridgett has extensive experience with helping clients develop and implement sound and defensible privacy, security and information retention and disposition policies that successfully balance our client's business objectives with their business, compliance and litigation-readiness needs. Hanson Bridgett

attorneys also have experience assisting clients with the development of incident response plans as well as guiding them through the legal issues that arise when an incident occurs. Outside counsel are essential members of an incident response team, providing legal risk analysis, representation and the umbrella of privilege for communications.

For more information, please contact:

Batya F. Forsyth, Partner
415-995-5827
bforsyth@hansonbridgett.com

William T. Kellermann, Counsel
415-995-5829
wkellermann@hansonbridgett.com