Published on *The National Law Review* https://natlawreview.com

FTC Asserts Data Security Authority without Need to Show Particularized Harm to Consumers

Article By:

Barbara Murphy Melby

Glen W. Rectenwald

In a recent FTC Opinion and Final Order relating to charges of unfair trade practices against a medical testing laboratory based upon alleged data security violations, the FTC has asserted the authority to take data security enforcement action against companies under the FTC Act for their security practices regardless of whether the data security violations have caused actual financial or physical harm to particular consumers.

The FTC Act prohibits unfair methods of competition in commerce. In a significant 2015 ruling on the FTC's authority, the US Court of Appeals for the Third Circuit upheld the general authority of the FTC to regulate cybersecurity under Section 5 (the unfairness prong) of the FTC Act. The court stated that under the amendments to the act, the FTC could deem a cybersecurity practice unfair if the practice causes or is likely to cause "substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."

In its recent order, the FTC reasserted its authority to regulate data security practices with a more expansive statement of the meaning of "substantial injury" in the cybersecurity realm: The privacy harm resulting from the unauthorized disclosure of sensitive health or medical information *"is in and of itself a substantial injury*" under the unfairness prong of the FTC Act. The FTC accordingly concluded that its enforcement actions based upon unreasonable data security practices do not need to show specific harm to particular consumers in order to prove "substantial injury" to consumers. Such unreasonable security practices may be shown to cause "substantial injury" based only on the deficiencies of the practices and the sensitivity of the information exposed.

If the FTC's order stands, it may prompt changes to the way companies assess data security risks, as the FTC could take action against deficient data security practices even without evidence that specific consumers have been harmed by those practices, particularly where highly sensitive information such as health and medical information is exposed. The order also highlights the need to consider the potentially expanded risk of FTC enforcement actions when allocating risks and responsibilities for data breaches in outsourcing and other complex commercial agreements.

In addition, as we discussed in a prior post, companies should continue to take care in crafting the terms of their privacy policies to ensure that the promises made in those policies are reasonably complete and accurate and are not deceptive. Companies should closely monitor guidelines that the FTC issues about protecting personally identifiable information and the latest security settlements and consent orders published by the FTC in order to ensure that the security practices remain consistent with FTC standards.

National Law Review, Volume VI, Number 216