CARLTON FIELDS

The FTC, Privacy, and the Life & Health Business

July 01, 2015

The Federal Trade Commission Act[1] ("FTC Act") prohibits unfair or deceptive acts or practices affecting commerce, as well as unfair competition in commerce.[2] The FTC Act also created the Federal Trade Commission ("FTC"), and authorized it to, among other things, prescribe rules defining specific acts or practices which are unfair or deceptive acts or practices in or affecting commerce, and to prevent persons, corporations and other entities (excluding banks, credit unions, common carriers, and other specific industries), from using unfair or deceptive acts or practices "in or affecting commerce."[3] The FTC Act also prohibits the dissemination of false advertisements by mail or other means in commerce, "for the purpose of inducing or which is likely to induce, directly or indirectly the purchase of …. services," and, defines the dissemination of such false advertisements as an "unfair or deceptive act or practice".[4] The FTC is authorized to bring actions in Federal Court to enforce the FTC Act, and may seek and obtain injunctive relief, restitution, and monetary penalties for violations.[5] The FTC Act does not exclude insurance from its scope as it does certain other enumerated industries (e.g., banks and savings and loans). Although the McCarran-Ferguson Act ("McCarran-Ferguson")[6] provides for state regulation of the "business of insurance" and generally prohibits federal laws from invalidating or superseding state laws regulating "the business of insurance," McCarran-Ferguson expressly provides that the FTC Act is applicable to "the business of insurance" to the extent that "such business" is not regulated by state law.[7] Thus, rather than exempting insurance companies from the reach of the FTC Act, McCarran-Ferguson exempts only those activities that constitute "the business of insurance," and then, only to the extent that such activities are regulated by state law. Therefore, in determining applicability of the FTC Act and FTC rules to an insurer, an "activity-based" analysis is required, starting with an inquiry into whether the specific activity by the insurer constitutes "the business of insurance". Whether McCarran-Ferguson removes an insurance business-related activity from FTC coverage then depends on the extent to which state law regulates that specific insurance activity, and whether enforcement of the FTC Act, and by extension, certain FTC rules, conflict with, or would in effect supersede, such state laws. With respect to privacy laws, the FTC also enforces the Fair Credit Reporting Act ("FCRA"), which applies directly to insurance, as well as the Gramm-Leach-Bliley Act ("GLB"), although the FTC is not

authorized to enforce GLB with respect to insurance, as well as the Children's Online Privacy Protection Act. As evidenced by its aggressive enforcement activities, the FTC is focusing on privacy and data security and it has taken the position that inadequate data security can be an unfair practice in violation of the FTC Act. The FTC's authority to establish data security standards for the private sector has been challenged by Wyndham Hotels & Resorts, LLC et al. ("Wyndham") in a pending FTC action against it, although the company's motion to dismiss the complaint on those grounds was denied and is now on appeal to the Third Circuit. The FTC contends that it has determined that "inadequate data security can be an 'unfair practice,'" within the meaning of the FTC Act, that it is authorized to make such a determination, and cites to the fact that it has issued more than 20 complaints charging deficient data security as unfair practices.[8] It seems unlikely that the Third Circuit will disagree with the FTC's position as to its authority to make such a determination generally, even if it is ultimately found that Wyndham's data security measures were not in fact so inadequate as to constitute unfair practices.[9] Relevant to the life and health insurance industry, the GLB requires standards for maintaining the privacy and security of non-public consumer information and applies to the industry, but these standards are supposed to be implemented by state laws. To the extent that states have enacted NAIC model GLB laws aligning with GLB requirements governing the treatment of non-public personal health and financial information by licensees (or other laws providing equivalent data security protection applicable to insurers), the FTC is unlikely to pursue insurance companies for data security or privacy violations. That said, the FTC may pursue service providers or industry partners who are not subject to state insurance regulations, and/or pursue a company in a state where regulation is lacking. FTC authority of principal concern for the life and health industry should continue to be the FCRA and its implementing regulations enforced by the FTC, including restrictions on sharing consumer information with affiliates for marketing purposes, and also, the risk that information obtained from data brokers, third party marketing companies, and other third party sources might be viewed by the agency as a "consumer report," leading to imposition of FCRA "user" duties, including provision of adverse action notices and disposal requirements for consumer reports.

---

[1] 15 U.S.C. § 41, et seq. "Commerce" means commerce among the states or with foreign nations, or in any territory of the United States or in the District of Columbia. 15 U.S.C. § 44 - Definitions [2] 15 U.S.C. § 45 [3] Id. [4] 15 U.S.C. § 52 [5] 15 U.S.C. § 45 [6] 15 U.S.c. § 1011, et seq. [7] 15 U.S.C. § 1012 [8] https://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation [9] As explained by Wyndham in its filings, despite what it contends were appropriate security measures, its systems were hacked by sophisticated cyber criminals. In deference to Wyndham's contentions, given the ever increasing sophistication of hackers, it should not be the case that every time a company's data is hacked, it must be concluded that its security measures were inadequate and unfair.

Related Practices

Cybersecurity and Privacy

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.