Clients&FriendsAlert

U.S. District Court Confirms FTC Authority to Regulate Corporate Data Security Practices

April 11, 2014

On April 7, 2014, Judge Esther Salas of the U.S. District Court for the District of New Jersey denied the first ever motion to dismiss filed in Federal court that challenged the authority of the Federal Trade Commission ("**the FTC**") to regulate corporate data security practices under section 5(a) of the Federal Trade Commission Act (the "**Act**"). The ruling came as part of the ongoing litigation between the FTC and Wyndham Worldwide Corporation and its subsidiaries, including Wyndham Hotels and Resorts ("**Wyndham**"). Specifically, the District Court rejected Wyndham's argument that the FTC lacked authority under section 5(a) of the Act to bring a complaint alleging that Wyndham's "failure to maintain reasonable and appropriate data security for consumers' sensitive personal information" was an "unfair" or "deceptive" business practice.[1] *FTC v. Wyndham Worldwide Corp.*, No. 13-1887, 2014 WL 1349019, at *3 (D.N.J. Apr. 7, 2014). In so deciding, the District Court has solidified the FTC's role as the leading Federal enforcer pushing businesses to adopt tighter cybersecurity measures to protect consumer data.

Wyndham offered two main arguments based on the United States Supreme Court's decision in *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000), in support of its motion to dismiss the FTC's complaint. In *Brown & Williamson*, the Supreme Court held that the FDA lacked the authority to regulate tobacco products because such an exercise of authority would be incompatible with the "overall regulatory scheme" created by Congress. *Id.* at 126. The Court explained that Congress expressed through tobacco-specific legislation an intent to "clearly preclude[] the FDA from asserting jurisdiction to regulate tobacco products." *Id.* In reaching its decision, the Court noted that the FDA had also "expressly disavowed any such authority since its inception . . . ." *Id.* Analogizing from *Brown & Williamson*, Wyndham contended that the "overall statutory landscape" created by Congress in the data security area preempts the FTC from using

[1] The District Court also rejected Wyndham's three other arguments in support of its motion to dismiss. First, the District Court disagreed with Wyndham's contention that the FTC is required to promulgate regulations that would provide fair notice of what "data-security practices the Commission believes Section 5 to forbid or require." *FTC v. Wyndham Worldwide Corp.*, No. 13-1887, 2014 WL 1349019, at *9 (D.N.J. Apr. 7, 2014). Second, the District Court held that the FTC's complaint sufficiently pleads an unfairness claim under the FTC Act. *See id.* at *16. Third, the District Court rejected Wyndham's argument that the FTC failed to state a deception claim. *See id.* at *22.

its authority under section 5(a) to establish and enforce private sector data security standards. *Wyndham*, 2014 WL 1349019 at *4. Second, Wyndham argued that, like the FDA, the FTC has "disclaimed authority" to regulate data security practices. *Id.* at *5. To support the contention, Wyndham identified three statements made by the FTC between 1998 and 2001 that suggest that the FTC believed it lacked the authority to regulate corporate data security. *See id.* at *7-8.

The District Court was not persuaded by either argument, characterizing Wyndham's position to be an "invitation to carve out a data-security exception to the FTC's unfairness authority . . . ." *Id.* at *6. First, the District Court stated that *Brown & Williamson* is distinguishable and emphasized that the Supreme Court had held that the FDA's exertion of authority over tobacco products "would *contradict* Congress'[s] clear intent" to deny the FDA such authority. *Id.* at *7 (quoting *Brown & Williamson*, 529 U.S. at 143) (emphasis added). Wyndham, according to the District Court, failed to "explain how the FTC's unfairness authority over data security would lead to a result that is incompatible with more recent [data security] legislation or would 'plainly *contradict* congressional policy.'" *Id.* at *6 (quoting *Brown & Williamson*, 529 U.S. at 139) (emphasis added). Indeed, the District Court said that "subsequent data-security legislation seems to complement—*not preclude*—the FTC's authority," which can "coexist with the existing data-security regulatory scheme." *Id.* at *7 (emphasis in original). Second, the District Court was "not convinced" that the three representations made by the FTC between 1998 and 2001 "equate to a resolute, unequivocal position under *Brown & Williamson* that the FTC has *no* authority to bring *any* unfairness claim involving data security." *Id.* at *8 (emphasis in original). The District Court added that the "public record here is unlike the lengthy, forceful history of repeated and consistent disavowals in *Brown & Williamson*." *Id.*

Given that the FTC—for more than a decade—has cited its section 5(a) authority as the basis for its enforcement actions against companies for their data security failures, the District Court's ruling should not be seen as a seismic shift in the cybersecurity regulatory enforcement landscape. Nevertheless, the decision may reinforce the FTC's view that it is effectively "the only game in town" with respect to Federal efforts to ensure the cybersecurity of U.S. businesses. The District Court's bolstering of the FTC's authority in the cyber realm, therefore, may lead the Commission to adopt an even more aggressive regulatory approach. Businesses that handle or maintain consumer data or other personally identifiable information must ensure that they have in place "reasonable" data security practices, because, as the FTC argued here, "reasonableness is the touchstone" and "unreasonable data-security practices are unfair" under the FTC Act. *Id.* at *10. Companies attempting to determine whether their data security practices are reasonable should look to industry

best practices, FTC's business guidance brochures,[2] and consent orders and complaints from previous FTC enforcement actions.[3]

* * * * *

If you have any questions, please contact any of the following attorneys or your Cadwalader contact:

Kenneth L. Wainstein	+1 202 862 2474	ken.wainstein@cwt.com
Peter E. Moll	+1 202 862 2220	peter.moll@cwt.com
Peter J. Isajiw	+1 212 504 6579	peter.isajiw@cwt.com
Keith M. Gerver	+1 202 862 2381	keith.gerver@cwt.com

[2] *See* Federal Trade Commission Bureau of Consumer Protection Business Center (April 10, 2014), *Data Security*, http://www.business.ftc.gov/privacy-and-security/data-security;

[3] *See, e.g.*, In the Matter of HTC America, Inc., In the Matter of Dave & Buster's, Inc., and In the Matter of LabMD, Inc.