New Ruling Challenges FTC Authority to Regulate Cybersecurity Based on "Possible Consumer Harm"

A Nov. 13, 2015 ruling supports the argument that various companies and lawyers have been making for years: the Federal Trade Commission is exceeding its authority in prosecuting cybersecurity breaches under Section 5 of the Federal Trade Commission Act.

In a decision that spans more than 90 pages, Judge D. Michael Chappel, the Chief Administrative Law Judge ("ALJ") for the Federal Trade Commission ("FTC" or "Commission"), issued his Initial Decision dismissing the FTC's Complaint against LabMD, Inc. ("LabMD"). In his ruling, the ALJ concluded that showing that there is a mere possibility of consumer harm is insufficient to prove unfairness under Section 5(n) of the FTC Act. This finding is significant for numerous reasons, but chief amongst them is that it was the first cybersecurity ruling of its kind that analyzed the underlying authority that the FTC has been exercising. This decision can also have a significant impact on the FTC's powers in other consumer protection clauses under sections of the FTC Act.

The judge found that the FTC failed to "demonstrate a likelihood that LabMD's computer network will be breached in the future and cause substantial computer injury. While there may be proof of possible consumer harm, the evidence fails to demonstrate probable, i.e., likely, substantial consumer injury. Because the evidence fails to prove that Respondent's alleged unreasonable data security caused, or is likely to cause, substantial consumer injury, as required by Section 5(n) of the FTC Act, Respondent's alleged unreasonable data security cannot properly be declared an unfair act or practice in violation of Section 5(a) of the FTC Act. Accordingly, the Complaint must be DISMISSED."[1]

In rejecting the FTC's data security case against LabMD, Judge Chappell's opinion shines a light on the argument against the FTC's decade-long effort to establish itself as the nation's chief cybersecurity regulator. The judge's opinion calls into question the FTC's predicate legal theory of enforcement. Further, Judge Chappell suggested the case should have never been brought, and questioned the constitutionality of the FTC's approach to its data security cases.

UNDERLYING ALLEGATIONS IN THE ADMINISTRATIVE COMPLAINT

Two alleged security incidents related to the company's alleged failure to provide reasonable and appropriate security for personal information formed the basis for the FTC's Administrative Complaint against LabMD. The first alleged incident occurred in 2008, when a data security company informed LabMD that one of LabMD's insurance aging reports containing personal information was available through a peer-to-peer file-sharing application. The report allegedly contained personal information, such as names, dates of birth, Social Security numbers, current procedural terminology ("CPT") codes, and health insurance company names, addresses, and policy numbers, for approximately 9,300 patients of LabMD's physician clients. The second alleged incident occurred in 2012, when documents

containing personal information were found in the possession of individuals who subsequently pleaded "no contest" to identity theft charges.

The Complaint concludes that Respondent's alleged failure to employ "reasonable and appropriate" measures to prevent unauthorized access to personal data caused, or is likely to cause, substantial harm to consumers that is not reasonably avoidable by consumers or outweighed by benefits to consumers or competition, and therefore constitutes an unfair practice under Section 5 of the FTC Act.

JUDGE'S FINDINGS

- With respect to the first alleged incident, the judge determined that the evidence failed to prove that either (1) "the limited exposure of the [data] file has resulted, or is likely to result, in any identity-related harm" or (2) "embarrassment or similar emotional harm is likely to be suffered from the exposure." He ruled that if there was any harm associated with the incident, it would be subjective or emotional harm, which is insufficient to constitute "substantial injury," as required to meet the standard of proof in Section 5(n) of the FTC Act, in the absence of evidence of any tangible injury.[2]
- With respect to the second alleged incident, the judge determined that the FTC failed to establish a causal connection between the incident and any failure on the company's part to reasonably protect data on its computer networks.
- Finally, the judge rejected the FTC's "argument that identity theft-related harm is likely for all consumers whose personal information is maintained on LabMD's computer networks, even if their information has not been exposed in a data breach, on the theory that LabMD's computer networks are 'at risk' of a future data breach," because the evidence failed to "assess the degree of the alleged risk, or otherwise demonstrate the probability that a data breach will occur."[3]

TAKEAWAYS

Enforcement Actions Based on Alleged Inadequate Security: Judge Chappel's opinion questions whether enforcement actions based on inadequate security, without other evidence of the actual likelihood of consumer harm, is sufficient. While situations akin to this have been the basis for many consent judgments, depending on the final results here, we expect more companies will be less likely to accept the consent judgments.

Evidence of Consumer Injury: In LabMD, the judge found no evidence that the consumer suffered harm as a result of an alleged failure to employ reasonable security measures. Further, the judge did not accept the claim that possible harm was sufficient. The judge questioned the FTC's reliance on expert testimony, which "only theorizes how consumer harm could occur." This finding is particularly interesting in light of the current split in the courts regarding the type of consumer injury required to support standing in data breach class actions.[4]

LabMD is sure to impact the circuit split and discussion regarding standing in a data breach class action. Various data breach class action opinions have found that the "allegations of possible future injury are not sufficient" to establish standing, but that standing instead requires that harm be "certainly impending." *See, e.g., In re ZAPPOS.COM, Inc., Customer Data Security Breach Litigation*, 2015 WL 3466943 (D. Nev. *June 1, 2015*): *Lewert et al. v. P.F. Chang's China Bistro, Inc.*, 2014 WL 7005097 (N.D. Ill. Dec. 10, 2014). However, just a few months ago, the Seventh Circuit in the Neiman Marcus data breach case found that preventative costs that cardholders might incur "easily" qualify as concrete injuries sufficient for the plaintiffs to establish standing to sue. *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 694 (7th Cir. July 20, 2015).

CONCLUSION

While the FTC has already filed an appeal to the LabMD ruling, this initial decision serves as a potential new tool for companies fighting the FTC's regulatory reach.

At Brownstein Hyatt Farber Schreck, we work with our clients in developing compliance strategies and to protect them from regulatory and litigation risk. Please do not hesitate to contact us with any questions.

———

[1] *In the Matter of LabMD Inc.*, Docket No. 9357 (Nov. 13, 2015) at 88.
[2] *In the Matter of LabMD Inc.,* Docket No. 9357 (Nov. 13, 2015) at 13.
[3] *In the Matter of LabMD Inc.*, Docket No. 9357 (Nov. 13, 2015) at 13-14.
[4] Id. at 52-53.

Jonathan C. Sandler
Shareholder
jsandler@bhfs.com
310.564.8672
Los Angeles

Makan Delrahim
Shareholder
mdelrahim@bhfs.com
310.500.4607
Washington, D.C.
Los Angeles

Richard B. Benenson
Shareholder
rbenenson@bhfs.com
303.223.1203
Denver