WILMERHALE

ALJ Dismisses FTC's LabMD Complaint for Lack of Actual or Probable Consumer Harm from Cybersecurity Incidents

NOVEMBER 16, 2015

On Friday, November 13, Federal Trade Commission ("FTC" or the "Commission") Chief Administrative Law Judge ("ALJ") D. Michael Chappell issued an Initial Decision in *In the Matter of LabMD, Inc.* (FTC Docket No. 9357), dismissing the Commission's Complaint against LabMD, Inc. ("LabMD"), upon a finding that the FTC had failed to "demonstrate a likelihood that [LabMD's] computer network will be breached in the future and cause substantial computer injury."[1] The ALJ held that showing consumer harm is merely *possible* is insufficient to prove unfairness under Section 5(n) of the FTC Act.

Background

The FTC's Administrative Complaint against LabMD alleged two "security incidents," which the Commission's Complaint blamed on LabMD's alleged failure to provide reasonable and appropriate security for personal information. The first alleged incident asserted in the complaint occurred in 2008, when data security company Tiversa Holding Company informed LabMD that one of LabMD's reports containing personal information was available through a peer-to-peer file-sharing application.

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.

Opinion

With respect to the first alleged incident, the ALJ found that the evidence introduced by Commission Counsel 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 determined that even if there were any harm, 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]

Next, the ALJ concluded that the Commission Counsel had failed to prove a causal connection

between the second alleged incident and any failure of LabMD to reasonably protect data on its computer networks, because the Commission Counsel had failed to show the documents at issue had actually been maintained on, or taken from, those networks. ALJ Chappell further found that Commission Counsel had "failed to prove that this exposure has caused, or is likely to cause, any consumer harm."[3]

Finally, the ALJ rejected Commission Counsel'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."[4]

Next Steps and Implication

The Initial Decision is almost certainly not final, as Commission Counsel will likely appeal the decision to the full Commission, which will issue a final decision that could then be appealed by LabMD, if the Commission rules against LabMD, to the United States Court of Appeals for the DC Circuit. And the facts of the case here are certainly factually distinguishable from others (such as the enforcement action against Wyndham Hotels) where there has been a data breach and at least some alleged actual loss to consumers. However, this opinion is significant for a number of its findings.

Inadequate security alone is not enough. The opinion forcefully questions the FTC's practice of bringing enforcement actions based on alleged inadequate security alone, without evidence of the actual likelihood (rather than the mere possibility) of consumer harm. The FTC staff has brought such cases in the past, and several companies have entered into consent orders (often with burdensome third-party audit and other requirements) based on such allegations. This opinion calls such cases into doubt, and, at least while this Initial Decision is pending appeal, may discourage FTC efforts to bring such types of enforcement actions.

Allegations of consumer injury must be supported by evidence. The ALJ found no evidence of consumer harm as a result of LabMD's alleged failure to employ reasonable security measures, and found the Commission Counsel's response—that consumers may not discover they have been victims of identity theft, or that possible harm is sufficient—unsatisfactory. The ALJ noted the absence of any evidence of harm after the passage of many years, and Commission Counsel's reliance on expert testimony, which "essentially only theorizes how consumer harm could occur."[5] 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.[6]

Questions of fairness of the adjudicative process. The procedural history of this case was complex, and the Commission itself directly resolved a number of important issues prior to the case reaching the ALJ. The ALJ repeatedly suggested that the Commission's direct involvement in the adjudication, displacing the ALJ, raises questions about fairness of FTC administrative processes. Such blunt criticism on this issue, by the Commission's chief ALJ no less, is striking and unusual. His critique is also relevant to a broader ongoing debate about the adequacy and fairness of agency

enforcement actions brought before ALJs rather than in Article III courts.

---

[1] *In the Matter of LabMD Inc.*, Docket No. 9357 (Nov. 13, 2015) at 88, available here.

[2] *Id*. at 13.

[3] *Id*.

[4] *Id*. at 13-14.

[5] *Id*. at 52-53.

[6] For example, this past July, in the class action suit against Neiman Marcus following its payment card breach, the Seventh Circuit found that preventive costs that cardholders might incur, such as credit monitoring subscriptions and replacement card fees, "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). Prior to the Remijas decision, a number of district courts dismissed breach-related class actions, citing the holding in *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138 (2013), a non-breach related case which found that "allegations of possible future injury are not sufficient" to establish standing, but that standing instead requires that harm be "certainly impending"—a standard which those courts found had not been met in the data breaches cases. *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).

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770