FTC Case Against LabMD Dismissed Due to Lack of Harm

Thursday, November 19, 2015

This past Friday the 13th was not a lucky day for the **Federal Trade Commission (FTC)**. An Administrative Law Judge (ALJ) dismissed the FTC's data security enforcement proceeding against LabMD on the grounds that the FTC failed to demonstrate that LabMD's allegedly lax security measures were likely to cause substantial injury to consumers. A copy of the decision can be found here.

Article By   James R. Kalyvas
Chanley T. HowellEileen R. Ridley
Steven MillendorfFoley & Lardner LLP
Legal News Alert

Antitrust & Trade Regulation
Communications, Media & Internet
Litigation / Trial Practice
All Federal

Impact to Businesses

Although the decision will likely be appealed, the ruling provides ammunition to companies facing an actual or potential enforcement action as a result of deficient, or allegedly deficient, data security practices. LabMD became only the second company (Wyndham Hotels being the other) not to settle with the FTC when faced with a data security enforcement action. For years, the conventional wisdom was that the FTC did not have to meet as high of a standard with respect to demonstrating consumer harm as the standard private litigants have had to meet in recent years.

This decision brings the conventional wisdom into doubt by requiring a strong showing that the data security practices are likely — not just possible — to cause substantial harm to consumers, and the FTC will now need to show more than just embarrassment or other emotional harm. In addition to providing support for businesses facing an FTC action, it may also cause the FTC to "pump the brakes" a bit when considering when to bring enforcement actions based solely on alleged lax data security.

Summary of the Decision

The ALJ noted Section 5(n) of the FTC Act states that "[t]he Commission shall have no authority to declare unlawful an act or practice on the grounds that such act or practice is unfair unless [1] the act or practice causes or is likely to cause substantial injury to consumers [2] which is not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition." The FTC alleged that LabMD had not employed reasonable data security measures resulting in the exposure or potential exposure of sensitive personal information such as Social Security numbers and health insurance information.

The ALJ held that the FTC failed to carry its burden of proving that LabMD's alleged failure to employ reasonable data security constitutes an unfair trade practice because it failed to prove the first prong of the three-part test – that the alleged unreasonable conduct caused or is likely to cause substantial injury to consumers. For example, the evidence failed to prove that the limited exposure of the personal information has resulted, or is likely to result, in any identity theft-related harm. The ALJ further held that the FTC failed to show that embarrassment or similar emotional harm is likely to be suffered from the exposure of the personal information. Even if there were proof of such harm, it would constitute only subjective or emotional harm that, under the facts of the case, where there is no proof of other tangible injury, is not a "substantial injury" within the meaning of Section 5(n).

The evidence failed to demonstrate that exposure of certain personal information was causally connected to any failure of LabMD to reasonably protect data maintained on its computer network. The evidence failed to show that documents in question were maintained on, or taken from, LabMD's computer network, and that the exposure

of the information has caused, or is likely to cause, any consumer harm.

Lastly, the ALJ 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 been not exposed in a data breach, on the theory that LabMD's computer networks are "at risk" of a future data breach. The evidence failed to assess the degree of the alleged risk, or otherwise demonstrate the probability that a data breach will occur. To impose liability for unfair conduct under Section 5(a) of the FTC Act, where there is no proof of actual injury to any consumer, based only on an unspecified and theoretical "risk" of a future data breach and identity theft injury, would require unacceptable speculation and would vitiate the statutory requirement of "likely" substantial consumer injury.

Thus the ALJ concluded that, at best, the FTC has proven only the "possibility" of harm, but not any "probability" or likelihood of harm. Fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm that was submitted by the FTC.

Conclusion

As noted above, this decision challenges the conventional wisdom that the FTC has a lower standard to meet with respect to showing harm than private litigants. Under this decision the FTC must make a strong showing that the data security practices are likely to cause substantial harm. The possibility of harm and allegations of embarrassment or other emotional harm are not sufficient. The decision provides potential defenses for companies facing an FTC action based solely on allegedly lax data security practices, and it may also make the FTC less likely to bring such enforcement actions against companies without evidence of likely harm to consumers.

© 2019 Foley & Lardner LLP

Source URL: https://www.natlawreview.com/article/ftc-case-against-labmd-dismissed-due-to-lack-harm