FTC complaint dismissed in LabMD data security case

In August 2013 the US Federal Trade Commission ('FTC') filed an administrative complaint against medical company LabMD on the basis of alleged failings in regards to the security of personal information of patients on LabMD's computer network. In the latest development, on 19 November an Administrative Law Judge at the FTC dismissed the case against LabMD, in a move that has surprised some. Patricia Wagner, Member at Epstein Becker Green, discusses the background to the decision and the Judge's findings of fact.

On 28 August 2013, the FTC issued an administrative complaint against LabMD. In that complaint, the FTC alleged that LabMD "failed to provide 'reasonable and appropriate' security for personal information maintained on LabMD's computer networks […]."[1] As a result of that failure the FTC alleged that LabMD's conduct violated Section 5(a) of the FTC Act, as conduct that caused or was likely to cause substantial consumer injury[2]. The case proceeded to an administrative hearing in front of an Administrative Law Judge at the FTC (the 'ALJ'). On 19 November 2015 the ALJ issued his Initial Decision, dismissing the FTC's complaint against LabMD. In that dismissal, the ALJ held that the FTC failed to meet its burden in showing that the conduct of LabMD caused consumer harm or was likely to cause consumer harm[3]. Under the FTC processes, the ALJ's Initial Decision may be reviewed by the full Commissioners of the FTC upon the request of any party or upon the Commissioners' own motion. On 24 November 2015, the FTC filed a Notice of Appeal[4].

ALJ's findings of fact

In rendering his decision, the ALJ first determined the findings of fact. In those findings, the ALJ found that the events leading to the FTC's complaint dated back to 2008. In May of that year, LabMD was contacted by a data security company, Tiversa. Tiversa informed LabMD that a file containing the names, dates of birth, social security numbers, insurance information and other identifying information of patients (the 'Insurance File') was available through a peer-to-peer file sharing application. LabMD investigated the report, determined the cause of the issue, and mitigated the issue by removing the application from the single computer on which it resided. In addition LabMD continued to monitor peer-to-peer networks to determine if the Insurance File was available on those networks. LabMD personnel were never able to find the Insurance File on any peer-to-peer network[5]. Tiversa continued to contact LabMD in an attempt to sell Tiversa's security remediation services. During these contacts, Tiversa represented that individuals were continuing to search for and download the Insurance File. In July 2008 LabMD instructed Tiversa that any further communications should occur through LabMD's lawyers[6].

In 2007 the FTC began communications with Tiversa regarding information available on peer-to-peer networks. As a result of these discussions, the FTC was interested in obtaining more detailed information from Tiversa. In July 2009 the FTC issued a Civil Investigative Demand ('CID') on the Privacy Institute. The Privacy Institute was a company created by Tiversa for the purpose of receiving and responding to the CID. In response to the CID, the Privacy Institute provided the FTC with a spreadsheet containing the names of companies "whose information exposure met a threshold of exposing 100 individuals' personal information."[7] The list provided to the FTC included LabMD[8].

In 2012, another incident affected LabMD. In October of that year, paper documents from LabMD (the 'Sacramento Documents') were found in a home in Sacramento, California as a result of a police investigation. One of the detectives investigating that incident performed an internet search and discovered that the FTC was investigating LabMD. The Sacramento police then forwarded information related to the Sacramento Documents to the FTC. The Sacramento Documents were documents that included names and potential social security numbers of roughly 682 consumers. The information on the sheets dated back to 2007, 2008 and 2009. The FTC notified LabMD of the discovery of this information, and LabMD notified all of the consumers included on the Sacramento Documents[9].

The key witness at the administrative hearing

As the case proceeded through the administrative hearing, there was a slight delay until one of the defence witnesses was able to obtain prosecutorial immunity for his testimony. Once granted, that witness testified that Tiversa (through the activities of this witness) had manufactured evidence so that it appeared that the sharing of the Insurance File was more widespread than it actually was. In addition, the witness testified that he manipulated the information so that it appeared that the Insurance File had been accessed by known

identity thieves. The witness was a former employee of Tiversa. The ALJ found this individual to be a credible witness[10].

No evidence of harm or likely harm

In making its case, the FTC relied on Section 5(n) of the FTC Act. That section provides that a practice is 'unfair' if it 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by the consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'[11]

In his dismissal, the ALJ held that the FTC had failed to demonstrate that consumers had been harmed or were likely to be harmed. Rather than merely relying on statistical studies evaluating the likelihood of identity theft, the ALJ evaluated the veracity and applicability of those studies to the case at hand. One of the FTC's experts testified regarding the risk to consumers using a four factor risk analysis: 1) the nature of the information disclosed; 2) to whom the disclosure was made; 3) whether the information was actually acquired or viewed; and 4) whether the data is still available for misuse by others[12]. In applying this test to the information available in the Insurance File, the ALJ held that the evidence demonstrated that the Insurance File had not been accessed by multiple outside individuals. Instead the Insurance File had only been accessed by Tiversa, a professor with whom Tiversa was collaborating, and the FTC. As a result, the ALJ opined, "there is no contention, or evidence, that the foregoing persons or entities present a threat of harming consumers."[13]

In determining the standard for likely harm, the ALJ held that the standard for 'likely' "does not mean that something is merely possible. Instead, 'likely' means that it is probable that something will occur."[14] The FTC argued that consumers may not know they are victims of identity theft even when they receive notice of a breach of their personal information. In response, the ALJ stated that that assertion "does not explain why [the FTC's] investigation would not have identified even one consumer that suffered any harm as a result of LabMD's alleged unreasonable data security."[15] The ALJ further noted that the absence of such harm after the passage of so many years "undermines the persuasiveness of the [FTC's] claim that such harm is nevertheless 'likely' to occur."[16] "Fairness dictates that reality must trump speculation based on mere opinion."[17]

In his dismissal, the ALJ held that the FTC had failed to demonstrate that consumers had been harmed or were likely to be harmed

The ALJ also evaluated whether LabMD's failure to "reasonably secure" data on its network caused or was likely to cause consumer harm as a result of the events associated with the finding of the Sacramento Documents. The Sacramento Documents were day sheets, and during the relevant time period printed on a daily basis, but not saved electronically[18]. As a result, the ALJ found that the FTC had failed to demonstrate that the Sacramento Documents were taken from LabMD's computers, and therefore it would "require unacceptable and unsupported speculation to conclude that the Sacramento Documents were exposed because of LabMD's alleged unreasonable computer security."[19] Further, the ALJ stated that none of the FTC's experts actually evaluated the security of LabMD's systems, leaving no evidence of unreasonable security practices[20].

Conclusion

With the appeal by the FTC staff, this case will continue. However, the opinion of the ALJ is instructive. Rather than merely relying on statistical studies, the ALJ considered the reality of the situation before him. In doing so, he found persuasive that the passage of time without reports of harm (even in the face of a government investigation) was strong evidence that harm was not likely to occur - and focuses the analysis on probability rather than possibility.

Patricia Wagner Member
Epstein Becker Green, Washington DC
pwagner@ebglaw.com

1. In the Matter of LabMD Inc., a corporation, Dkt. No. 9357 (13 November 2015) (hereinafter 'Initial Decision') at 1-2.
2. Initial Decision at p.1.
3. Ibid. at 1.
4. https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter. In addition, LabMD filed a complaint in federal court against three of the FTC staff attorneys that worked on this case, alleging that they violated the First, Fourth, and Fifth Amendments and participated in a civil conspiracy.
5. Ibid. at 58.
6. Ibid. at 30.
7. Ibid. at 31.
8. Ibid. at 31-32.
9. Ibid. at 36-39.
10. Ibid. at 9, 33, 34.
11. Ibid. at 47.
12. Ibid. at 60-65.
13. Ibid. at 61.
14. Ibid. at 54.
15. Ibid. at 52.
16. Ibid.
17. Ibid. at 64.
18. Ibid. at 70-74.
19. Ibid. at 74.
20. Ibid. at 85.