Published on *The National Law Review* https://natlawreview.com

When Do Data Security Breaches Cause Substantial Consumer Harm? Lessons from the LabMD FTC Complaint Dismissal

Article By:

Patricia M. Wagner

On November 19, 2015, an Administrative Law Judge (the "ALJ") at the Federal Trade Commission ("FTC") dismissed the FTC's 2013 complaint against LabMD, a clinical testing laboratory, stating that the FTC failed to demonstrate that LabMD's conduct caused consumer harm or was likely to cause consumer harm.[1]

In the complaint against LabMD, the FTC had alleged that LabMD "failed to provide 'reasonable and appropriate' security for personal information maintained on LabMD's computer networks. . . ."[2] According to the FTC, that failure was a violation of Section 5(a) of the FTC Act, as it was conduct that caused or was likely to cause substantial consumer injury.[3]

Despite the convoluted and unique circumstances at issue in the LabMD case, the ALJ's Initial Decision provides a useful framework for assessing whether conduct "is likely" to cause substantial consumer harm—a gating question for agencies and courts evaluating many security breaches.

Background

Based on the findings of the ALJ, the background facts are as follows. The events leading to the FTC's complaint date back to 2008. In May of that year, LabMD was contacted by a data security company, Tiversa, which informed LabMD that a file containing 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 peer-to-peer application from the single computer on which it resided. In addition, LabMD monitored peer-to-peer networks to determine if the Insurance File was available on those networks. They were not able to find the Insurance File on any peer-to-peer network.[4]

Meanwhile, Tiversa continued to contact LabMD in an attempt to sell Tiversa's remediation services. During these contacts, Tiversa represented that individuals were continuing to search for and download the Insurance File. In July of 2008, LabMD instructed Tiversa that any further communications should occur through LabMD's lawyers.[5]

The FTC became aware of LabMD through Tiversa. In July 2009, the FTC issued a Civil Investigative Demand ("CID") on the Privacy Institute, a company created by Tiversa following prior communications with the FTC, for the sole purpose of receiving the CID. The CID requested the names of companies for which Tiversa had found public-facing documents containing at least 100 individuals' personal information. The list provided to the FTC included LabMD.[6]

A few years later, in October 2012, paper documents from LabMD were found in a home in Sacramento, California, as a result of a police

investigation there. The Sacramento police forwarded information related to that finding to the FTC. The so-called “Sacramento Documents” included nine photocopied checks and 40 sheets of paper listing the names and apparent 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.[7]

Both incidents—the events related to the Insurance File and to the Sacramento Documents—were included in the FTC’s complaint against LabMD. The FTC issued its complaint against LabMD on August 28, 2013.[8]

The Linchpin of the Administrative Hearing

The FTC’s case proceeded through to an administrative hearing. In a twist of events, a defense witness who had been granted prosecutorial immunity testified that while he was an employee of Tiversa, he had manufactured certain evidence so that it appeared the sharing of the Insurance File was more widespread than it actually was. In addition, he admitted that he had manipulated the information so that it appeared that the Insurance File had been accessed by known identity thieves. The ALJ found this witness credible.[9]

No Evidence of Harm or Likely Harm Related to the Insurance File

The FTC alleged that the failure to have appropriate security practices in place was an “unfair practice,” in violation of Section 5(a) of the FTC Act. In so doing, the FTC relied on Section 5(n) of the FTC Act, which 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."[10] The ALJ held that the FTC had not presented any evidence that any consumer suffered any harm as a result of LabMD's conduct.

The ALJ discounted the testimony of the FTC's expert witnesses, concerning the likelihood of consumer harm, as they (1) assumed that LabMD failed to provide adequate security and (2) relied on less than robust surveys and statistics. One of the experts evaluated the risk of personal harm by 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.[11] In applying this test, the ALJ held that because the evidence demonstrated that the Insurance File had not be accessed by multiple outside individuals—as originally suggested by Tiversa—but had only been accessed by Tiversa, a professor with whom Tiversa was collaborating, and the FTC, "there is no contention, or evidence, that the foregoing persons or entities present a threat of harming consumers."[12]

Importantly, the ALJ opined that historically, liability for unfair conduct has only been found in instances where there is proof of actual consumer harm. Thus, the ALJ held that the standard for "likely" to cause substantial injury to consumers **"does not mean that something is merely possible. Instead, 'likely' means that it is probable that something will occur."**[13] 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 the 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."[14] 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."[15]

Indeed, the ALJ noted that the FTC relied on a statistic that 30.5 percent of individuals notified of a breach report experience identity theft within 12 months of that event. Citing that statistic, the ALJ stated that "it would be expected that the government, in the many years of investigation and litigation of this matter, would have discovered and identified at least one such consumer who has experienced identity theft harm. … Fairness dictates that reality must trump speculation based on mere opinion."[16]

No Evidence of Harm or Likely Harm Related to the Sacramento Documents

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 discovery of the Sacramento Documents.

The Sacramento Documents were day sheets, which LabMD printed on a daily basis. Once printed, the documents were not saved electronically. Since LabMD didn't start to scan and save these day sheets until January 2013, the ALJ found that the FTC had failed to demonstrate that the Sacramento Documents—discovered in October 2012[17]—were taken from LabMD's computers, and that therefore, it would "require unacceptable and unsupported speculation to conclude that the Sacramento Documents were exposed because of LabMD's alleged unreasonable computer security."[18]

In addition, the ALJ noted that the FTC's expert had opined that although

individuals affected by the Sacramento Documents event had been offered credit monitoring, they still faced a "strong possibility" of becoming identity theft victims. To this, the ALJ stated that the expert's opinions "describe little more than the possibility of future harm, or an unquantified inchoate 'risk' of future harm."[19]

As proof of harm, the FTC introduced a document that purported to demonstrate that the social security numbers listed on the Sacramento Documents had been used by people with different names. This, the FTC claimed, demonstrated that the social security numbers had been used by identity thieves. However, the ALJ held that the FTC had failed to demonstrate the authenticity or reliability of the information included in the spreadsheet, which was created using a third-party service. As a result, the ALJ held that the spreadsheet was inadmissible and therefore could not be used as proof of consumer harm. Further, the ALJ stated that none of the FTC's experts actually evaluated the security of LabMD's systems and left "virtually no evidence to support the contention that LabMD's alleged unreasonable security practices are likely to cause harm to consumers. . . ."[20]

Next Steps

Under the FTC processes, the ALJ's decision (deemed the Initial Decision) may be reviewed by the full Federal Trade Commission upon the request of any party or upon the Commission's own motion. On November 24, 2015, the FTC filed a Notice of Appeal.[21]

Key Takeaways

As noted above, despite the unique and convoluted facts associated with this case, the ALJ's opinion provides guidance for agencies and courts

evaluating data security breach incidents.

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. Further, the ALJ refused to be swayed by arguments that if identity theft is *possible,* the harm is therefore *likely* to occur. Rather, not only did the ALJ hold that possibility is not the appropriate standard (rather it is one of probability), he found it 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.

[1] In the Matter of LabMD Inc., a corporation, Dkt. No. 9357 (November 13, 2015) (hereinafter “Initial Decision”).

[2] Initial Decision at p.1.

[3] *Id.*

[4] *Id.* at 58.

[5] *Id.* at 30.

[6] *Id.* at 31-32.

[7] *Id.* at 36-39.

[8] *Id.* at 1-2.

[9] *Id.* at 9, 33, 34.

[10] *Id.* at 47.

[11] *Id.* at 60-65.

[12] *Id.* at 61.

[13] *Id.* at 54.

[14] *Id.* at 52.

[15] *Id.*

[16] *Id.* at 64.

[17] *Id.* at 70-74.

[18] *Id.* at 74.

[19] *Id.* at 75.

[20] *Id.* at 85

[21] See https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter. In addition, LabMD has sued 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

National Law Review, Volume V, Number 336