Cooley

November 23, 2015

Federal Trade Commission ("FTC") charges against the cancer-screening laboratory LabMD, stemming from two data breaches involving sensitive personal information of thousands of consumers were dismissed in a decision made public last week by an FTC administrative judge given the lack of evidence of actual or likely harm to consumers.

The FTC alleged in August 2013 that LabMD engaged in "unfair" trade practices under the Federal Trade Commission Act ("FTC Act"), asserting that the company failed to reasonably protect the security of consumers' personal data, including medical information, on LabMD computer systems.[1] In a 92-page decision, the administrative law judge ("ALJ") dismissed the action, holding that the FTC staff had proven only a "possibility of harm" and not the "probability" or "likelihood" of harm that the FTC Act requires.

The case stems from events in 2008 when a third-party security consulting firm informed the FTC that a LabMD insurance billing spreadsheet containing sensitive patient information was available on the peer-to-peer ("P2P") file-sharing network, LimeWire. The spreadsheet contained patient names, Social Security numbers, and birthdates, as well as health insurance provider information and standardized medical treatment codes.

A second security incident was alleged to have occurred in 2012 involving documents that were found in the possession of individuals that subsequently pleaded no contest to identity theft charges. The documents included personal information such as names and Social Security numbers used by the identity thieves.

The FTC investigated and brought an administrative complaint against LabMD under Section 5 of the FTC Act alleging that LabMD engaged in "unfair" practices by failing to take reasonable and appropriate measures to prevent unauthorized disclosure of sensitive patient data on its networks. Section 5(a) of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." Section 5(n) outlines the standard of proof and provides that a practice can only be deemed "unfair" if it "causes or is *likely to cause substantial* injury to consumers."

Unfairness also requires that such injury not be reasonably avoidable by consumers themselves, and required that the injury not be outweighed by countervailing benefits to consumers or to competition, issues not present in this case since the judge found there was insufficient evidence to support the complaint.

The ALJ dismissed the action in connection with the 2012 incident finding that there was no evidence that any alleged failure to reasonably secure LabMD's computer networks caused the exposure of the documents. There was no evidence that the materials found in the hands of identity thieves were sourced from LabMD's computer networks. While the documents could be traced to LabMD, there were many ways that the documents could have been obtained and no support for the fact that a failure in computer security was the source.

In dismissing the action in connection with the 2008 incident, the ALJ found that the 5(n) standard of actual or likely injury was not met as the record contained no evidence of identity theft or other actual harm and only a "possibility of harm." The ALJ's decision turned heavily on evidence that no one, other than LabMD and the security consulting firm that reported the incident, had actually accessed the exposed insurance report. The FTC staff retreated from other proferred evidence after discovering that a security firm had falsified data relied upon by FTC experts, purporting to show that compromised LabMD files had spread to IP addresses of known identity thieves.

Importantly, the ALJ also held that a consumer's "embarrassment or other emotional harm," inflicted by exposure of sensitive information on a P2P network was only a "subjective harm" and did not amount to a "substantial injury" within the meaning of Section 5(n) where there was no proof of other tangible injury.

Finally, the judge rejected the FTC staff's theory that *all* consumers whose data was stored on LabMD's network faced a "likely risk" of identity theft, reasoning that the FTC's evidence of security weaknesses failed to adequately assess the degree of risk or probability that a future breach would occur. The ALJ concluded, "[t]o 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 statutory requirement of 'likely' substantial consumer injury."

LabMD's victory could be short-lived as the FTC staff can appeal the ALJ's decision to the full FTC, which will review the record de novo.

Even if the FTC Commissioners reverse the ALJ decision, they will be forced to articulate a standard for "likely substantial harm" that will guide future Section 5(n) jurisprudence. The agency's final decision will be reviewable by the U.S. Court of Appeals.

If the ALJ's decision is upheld, either by the full Commission or an appellate court, the outcome will align FTC enforcement more closely with the standards of Article III "injury in fact" that private litigants must meet in data breach cases to have standing to sue in federal court.

In the short run, the ALJ decision can be expected to have an immediate impact, leading the FTC staff to be more cautious before bringing enforcement actions in data security cases where there is no record of actual consumer harm. It will likely also embolden other companies to stand up and fight where there is not evidence of actual or likely consumer injury rather than accept FTC consent decrees that typically impose 20-year security auditing and reporting obligations.

Notes

1. The FTC alleged that LabMD's security failures included, among other things, that they:
   (a) did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information;
   (b) did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks;
   (c) did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;
   (d) did not adequately train employees to safeguard personal information;
   (e) did not require employees, or other users with remote access to the networks, to use common authentication-related security measures;
   (f) did not maintain and update operating systems of computers and other devices on its networks; and
   (g) did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks.

Key Contacts

Matthew D. Brown San Francisco	brownmd@cooley.com +1 415 693 2188

Howard Morse Washington, DC	hmorse@cooley.com +1 202 842 7852
Scott Dailard San Diego	sdailard@cooley.com +1 858 550 6062
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090