Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Key Data Security Takeaways From LabMD

Law360, New York (August 16, 2016, 12:28 PM ET) --
On July 29, 2016, the Federal Trade Commission announced its long-awaited decision in its LabMD enforcement action. The commissioners reversed the decision of an administrative law judge and held that LabMD engaged in "unfair" practices in violation of Section 5 of the FTC Act because LabMD unreasonably failed to protect the security of consumers' sensitive medical and personal information.


Bethany C. Lobo


Matthew D. Brown


Howard Morse

The commission's decision is notable for two key holdings:

- A company's mere public exposure of sensitive consumer information can constitute a substantial consumer injury supporting a Section 5 "unfairness" violation, without evidence that anyone ever misused the consumer information.

- A company may violate Section 5's prohibition on "unfair" practices if its data security practices risk a consumer injury of large magnitude, even if the likelihood of the injury occurring is low.

The LabMD decision marks one of the first times that the FTC has ruled on the scope of its data security enforcement authority in an administrative proceeding. Because LabMD has vowed to appeal, the case will likely prompt important judicial guidance on whether the FTC Act authorizes the FTC to find that companies whose allegedly deficient data security practices have not caused any consumers actual or imminent harm have violated Section 5.

The FTC's Administrative Complaint Against LabMD

From 2001 to 2014, LabMD was a clinical laboratory that tested patient specimen samples provided by physicians throughout the United States. One of its employees installed LimeWire, peer-to-peer file-sharing software, on her work computer to download music. She publicly shared numerous files via LimeWire, apparently inadvertently including a LabMD insurance billing spreadsheet that contained 9,300 patients' Social Security numbers, birth dates, medical diagnosis codes, physician orders for tests and services, and insurance policy information. In 2008, third-party data security company Tiversa advised LabMD that it had downloaded the billing spreadsheet from LimeWire. Tiversa repeatedly tried to sell

LabMD its remediation services. When unsuccessful, Tiversa provided the LabMD billing spreadsheet and other evidence related to LabMD's data security practices to the FTC.[1]

In 2013, the FTC issued an administrative complaint alleging that LabMD violated Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair and deceptive acts or practices in or affecting commerce." The FTC's complaint alleged that the LimeWire incident illustrated that LabMD's data security practices were "unfair" under Section 5. Rather than enter a consent agreement (as most companies do), which would have required it to agree to adopt data security practices and conduct periodic audits, LabMD decided to make the FTC prove its case on the merits.

The ALJ's Initial Decision

In November 2015, the ALJ dismissed the case after a trial, finding that the FTC's complaint counsel had not met their burden of proof. Section 5(n) of the FTC Act requires a three-pronged showing in an "unfairness" action: (1) the disputed business practice has caused or is likely to cause substantial injury to consumers (2) which the consumers cannot reasonably avoid and (3) that is not outweighed by countervailing benefits to consumers or competition.

The ALJ addressed only the first prong, holding that complaint counsel failed to prove that LabMD's data security practices had caused consumers any nonhypothetical or nontheoretical harm. The ALJ found that LabMD's data security practices did not "cause" substantial consumer injury, where there was no evidence that anyone ever misused the consumers' data.

Defining "likely to cause" as "having a high probability of occurring or being true," the ALJ held that complaint counsel had not shown that LabMD's data security practices were "likely to cause" substantial consumer injury. The ALJ reasoned that such injury was improbable where no consumers had complained of injury linked to the spreadsheet's disclosure, and there was no evidence that anyone other than Tiversa had ever downloaded the spreadsheet from LimeWire.

The FTC's Opinion and Final Order Reversing the ALJ's Initial Decision

Complaint counsel appealed to the full commission, which — with only three sitting commissioners — reversed the ALJ and held, reviewing the facts de novo, that the required three-pronged unfairness showing was met.

1. The challenged practice caused, or is likely to cause, substantial injury to consumers.

- The commission concluded that LabMD's data security practices "caused" substantial injury because they allowed an employee to run LimeWire undetected for three years, causing the exposure of the insurance billing spreadsheet. The commissioners concluded that public exposure of a spreadsheet containing sensitive health and medical data was itself a substantial injury.

- The commission rejected the ALJ's holding that the "likely to cause" standard required a showing that a substantial consumer injury was "probable." Instead, the commissioners reasoned that there only needed to be a "significant risk" of consumer injury, and one could look to the likelihood or probability of the injury occurring and the magnitude or seriousness of the injury if it does occur.

> Thus, a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low.

According to the commissioners, LabMD's data security practices were likely to cause substantial injury, even though not one consumer had reported any injury in the many years since the insurance billing spreadsheet was exposed. The absence of such reports was not dispositive, according to the commissioners, because LabMD did not notify consumers of the breach, and absent notification, consumers often do not learn that a company has exposed their personal information (let alone which company). Here, the FTC reasoned, the magnitude of the potential harm was high due to the sensitivity of the compromised medical data.

2. Consumers could not reasonably avoid the injuries resulting from LabMD's data security practices.

The commission held that consumers could not avoid the injury caused by LabMD's exposure of their sensitive data. The commissioners reasoned that patients provided samples to their physicians for testing; most did not even know that their samples were provided to LabMD, and they lacked any information about LabMD's data security practices. Thus, they could not have avoided any injury caused by those practices.

3. The injuries to consumers were not outweighed by countervailing benefits to consumers or competition.

The commission held that complaint counsel satisfied this third prong because LabMD's deficient data security practices produced adverse consequences for consumers that were not accompanied by an increase in services or benefits to consumers or benefits to competition. The commissioners reasoned that this was particularly true given the availability of relatively low-cost solutions including risk management techniques (e.g., penetration-testing programs or file-integrity monitoring tools), employee training, data minimization policies, and administrative limitations on employees' network access.

After concluding that the three "unfairness" requirements were met,[2] the commissioners also rejected LabMD's affirmative defense that the enforcement action violated due process because LabMD lacked adequate notice of what data security practices are required by Section 5. The commissioners asserted that the FTC had provided adequate guidance as to reasonable and appropriate data security practices in its complaints, administrative decisions, and consent decrees.

The commissioners ordered LabMD to take three remediation measures:

- Establish a comprehensive information security program to protect the security and confidentiality of consumers' data in its possession.
- Submit to third-party security audits for 20 years.
- Notify affected consumers about the unauthorized disclosure of their personal information and how they can protect themselves from identity theft or related harms; provide copies of these notices to the consumers' health insurers.

These requirements are similar to those that LabMD would have faced if it had settled early on with the FTC rather than litigating through trial and appeal to the full commission.

LabMD now has until late September to file a petition for review of the FTC's order with a U.S. Court of Appeals. LabMD's CEO, Michael Daugherty, has said the company will appeal.

Practical Considerations

1. Companies may continue to settle with the FTC rather than challenge enforcement actions.

Since 2002, the FTC has brought more than 50 data security enforcement actions under Section 5 of the FTC Act.

Most companies faced with an FTC enforcement action swiftly enter consent decrees requiring them to take remediation measures similar to those described above. Only two companies — LabMD and hotelier Wyndham Worldwide Corporation — have litigated the FTC's data security enforcement authority under Section 5's "unfairness" prong. Wyndham settled with the FTC after the Third Circuit rejected its challenge to the FTC's "unfairness" enforcement authority, and LabMD has now lost before the commission. LabMD has paid a high price for its choice to litigate: as a small company, it could not withstand the reputational harms and financial costs of fighting the FTC, and wound down its operations in early 2014.[3] Unless LabMD prevails on appeal (and even if it does), its story may leave companies eager to settle with the FTC rather than litigate.

2. The FTC may bring more enforcement actions without evidence of consumer harm.

Some have been surprised that the FTC pursued this enforcement action without any evidence that the consumer data was even accessed by a bad actor — let alone actually misused by one. If the LabMD decision is upheld on appeal, the FTC will likely feel empowered to continue to bring data security enforcement actions even where it lacks evidence of actual or imminent consumer harm.

3. The FTC may continue to bring data security enforcement actions against HIPAA-governed entities.

The FTC acknowledged that LabMD was a covered entity under the Health Insurance Portability and Accountability Act of 1996, yet maintained this Section 5 enforcement action even though HIPAA contains its own data security standards tailored to the health care industry, which are enforced by the U.S. Department of Health and Human Services. The FTC can be expected to continue to bring Section 5 actions against health care providers notwithstanding HIPAA.

4. The FTC's interpretation of "unfair" conduct may affect interpretation of state unfair competition laws modeled on the FTC Act.

Many states have "little FTC Acts" modeled on the FTC Act, which prohibit companies from engaging in unfair business acts. These statutes authorize enforcement by state attorneys generals, and sometimes by private citizens. AGs and private plaintiffs may invoke the FTC's decision to argue against dismissal of claims under little FTC Acts, in cases where they are hard-pressed to identify any actual or imminent consumer harm.

5. Litigants in consumer class actions will undoubtedly debate the relevance of the FTC's decision to

Article III standing inquiries.

Following a data breach, companies often face class actions from consumers whose data was potentially compromised. Many (but not all) federal courts have held that plaintiffs cannot establish standing to sue based on fears of future harm, unless they can show an actual misuse of their data. Although the FTC's order is not binding on the federal courts, litigants will likely debate its relevance to Article III standing. Plaintiffs may cite the FTC decision to support an argument that consumers are injured when their sensitive data is compromised, even absent evidence of actual misuse. But defendants will likely respond that the decision is irrelevant to an Article III standing analysis, because the commissioners rejected LabMD's argument that it is required to demonstrate that consumers suffered an injury-in-fact adequate to satisfy Article III standing requirements.

6. Companies should evaluate the adequacy of their data security practices.

Companies should evaluate the adequacy of their data security practices in light of the LabMD decision and the FTC's published guidance, complaints and settlements. A good place to start is the FTC's June 2015 publication, "Start with Security," which provides 10 data security principles distilled from the FTC's 50-plus data security enforcement actions. Companies should also specifically consider adopting the data security measures encouraged in the LabMD order, including using risk management software, adequately training employees, adopting data minimization policies, and administratively limiting employees' network access.

7. Companies should also be careful about their public statements regarding their data security practices.

While the LabMD enforcement action was based entirely on the FTC's "unfairness" authority, companies should be aware that the FTC often challenges companies' statements regarding their data security practices as deceptive, following a data breach. Companies should review their public statements and be careful not to overstate their privacy and data security practices.

—By Bethany C. Lobo, Matthew D. Brown and Howard Morse, Cooley LLP

Bethany Lobo is a senior associate and Matthew Brown is a partner in Cooley's San Francisco office. Howard Morse is a partner in the firm's Washington, D.C., office and previously served at the Federal Trade Commission as deputy assistant director for policy and assistant director of the FTC's Bureau of Competition.

[1] Because Tiversa falsified some of the evidence against LabMD that it provided to the FTC, complaint counsel ultimately disclaimed reliance on most of Tiversa's evidence.

[2] Complaint counsel had also alleged a second data security failure: In 2012, California police arrested suspected identity thieves who possessed hard copies of LabMD documents containing hundreds of consumers' personal information, including Social Security numbers. However, the FTC affirmed the ALJ's dismissal of these allegations, explaining that the evidence established no causal connection between the exposed hard copy documents and LabMD's data security practices.

[3] The commissioners nonetheless maintained that their 2016 order was necessary because LabMD still maintains a computer system with approximately 750,000 consumers' data and may resume its operations in the future.
