[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 16-16270

Agency No. 9357

LABMD, INC.,

Petitioner,

versus

FEDERAL TRADE COMMISSION,

Respondent.

Petition for Review of a Decision of the
Federal Trade Commission

(June 6, 2018)

Before TJOFLAT and WILSON, Circuit Judges, and ROBRENO,* District Judge.

TJOFLAT, Circuit Judge:

---

* Honorable Eduardo C. Robreno, United States District Judge for the Eastern District of Pennsylvania, sitting by designation.

This is an enforcement action brought by the Federal Trade Commission ("FTC" or "Commission") against LabMD, Inc., alleging that LabMD's data-security program was inadequate and thus constituted an "unfair act or practice" under Section 5(a) of the Federal Trade Commission Act (the "FTC Act" or "Act"), 15 U.S.C. § 45(a).[1] Following a trial before an administrative law judge ("ALJ"), the Commission issued a cease and desist order directing LabMD to create and implement a variety of protective measures. LabMD petitions this Court to vacate the order, arguing that the order is unenforceable because it does not direct LabMD to cease committing an unfair act or practice within the meaning of Section 5(a). We agree and accordingly vacate the order.[2]

I.

A.

LabMD is a now-defunct medical laboratory that previously conducted diagnostic testing for cancer.[3] It used medical specimen samples, along with relevant patient information, to provide physicians with diagnoses. Given the nature of its work, LabMD was subject to data-security regulations issued under

[1] Section 5(a) declares unlawful "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1). It empowers and directs the Commission "to prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." *Id.* § 45(a)(2).

[2] *See* 15 U.S.C. § 45(c).

[3] LabMD is no longer in operation but still exists as a company and continues to secure its computers and the patient data stored within them.

the Health Insurance Portability and Accountability Act of 1996, known colloquially as HIPAA. LabMD employed a data-security program in an effort to comply with those regulations.[4]

Sometime in 2005, contrary to LabMD policy, a peer-to-peer file-sharing application called LimeWire was installed on a computer used by LabMD's billing manager.[5] LimeWire is an application commonly used for sharing and downloading music and videos over the Internet. It connects to the "Gnutella" network, which during the relevant period had two to five million people logged in at any given time. Those using LimeWire and connected to the Gnutella network can browse directories and download files that other users on the network designate for sharing. The billing manager designated the contents of the "My Documents" folder on her computer for sharing, exposing the contents to the other users. Between July 2007 and May 2008, this folder contained a 1,718-page file (the "1718 File") with the personal information of 9,300 consumers, including names, dates of birth, social security numbers, laboratory test codes, and, for some, health insurance company names, addresses, and policy numbers.

In February 2008, Tiversa Holding Corporation, an entity specializing in data security, used LimeWire to download the 1718 File. Tiversa began contacting

[4] LabMD's program included "a compliance program, training, firewalls, network monitoring, password controls, access controls, antivirus, and security-related inspections."

[5] The record is not clear on the point but we assume that the billing manager installed the peer-to-peer application on her workstation computer.

LabMD months later, offering to sell its remediation services to LabMD.[6] LabMD refused Tiversa's services and removed LimeWire from the billing manager's computer. Tiversa's solicitations stopped in July 2008, after LabMD instructed Tiversa to direct any further communications to LabMD's lawyer. In 2009, Tiversa arranged for the delivery of the 1718 File to the FTC.[7]

B.

In August 2013, the Commission, following an extensive investigation, issued an administrative complaint against LabMD and assigned an ALJ to the

---

[6] As described by the ALJ who initially presided over this case,

> [Tiversa's] efforts included representing to LabMD that the 1718 File had been found on a peer-to-peer network and sending LabMD a Tiversa Incident Response Services Agreement describing Tiversa's proposed fee schedule, payment terms, and services that would be provided. These contacts continued from mid-May through mid-July 2008. In these communications, Tiversa represented that Tiversa had "continued to see individuals [on peer-to-peer networks] searching for and downloading copies" of the 1718 File. . . .
>
> Tiversa's representations in its communications with LabMD that the 1718 File was being searched for on peer-to-peer networks, and that the 1718 File had spread across peer-to-peer networks, were not true. These assertions were the "usual sales pitch" to encourage the purchase of remediation services from Tiversa. . . .

Tiversa did, however, share a copy of the 1718 File with a Dartmouth College professor, who in February 2009 published an article about data security in the healthcare industry. Tiversa was a "research partner" for the article, meaning it searched for and provided the professor with relevant files to analyze. The professor did not share the 1718 File or its contents with anyone.

[7] Tiversa's CEO and the FTC offered testimony at a 2007 congressional hearing regarding peer-to-peer file-sharing technology. About two months after the hearing, the FTC and Tiversa began communicating. The FTC wanted Tiversa to provide it with information regarding companies' data-security practices. Tiversa, though, did not want a formal request for information—such as a Civil Investigative Demand ("CID")—to be issued directly to it because it had been in talks about its possible acquisition by a third party. Tiversa thus created an entity called "The Privacy Institute" so that a CID could be issued without directly implicating Tiversa. The FTC issued a CID to The Privacy Institute in 2009 and The Privacy Institute provided the FTC with the 1718 File.

case. The complaint alleged that LabMD had committed an "unfair act or practice" prohibited by Section 5(a) by "engag[ing] in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks." Rather than allege specific acts or practices that LabMD engaged in, however, the FTC's complaint set forth a number of data-security measures that LabMD failed to perform.[8] LabMD

---

[8] The FTC's complaint alleged that LabMD

(a) did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information. Thus, for example, employees were allowed to send emails with such information to their personal email accounts without using readily available measures to protect the information from unauthorized disclosure;

(b) did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks. By not using measures such as penetration tests, for example, respondent could not adequately assess the extent of the risks and vulnerabilities of 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, such as periodically changing passwords, prohibiting the use of the same password across applications and programs, or using two-factor authentication;

(f) did not maintain and update operating systems of computers and other devices on its networks. For example, on some computers respondent used operating systems that were unsupported by the vendor, making it unlikely that the systems would be updated to address newly discovered vulnerabilities; and

(g) did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks. For example, respondent did not use appropriate measures to prevent employees from installing on computers applications or materials that were not needed to perform their jobs or adequately maintain or review records of activity on its

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.