[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

answered the complaint, denying it had engaged in the conduct alleged and asserting several affirmative defenses, among them that the Commission lacked authority under Section 5 of the Act to regulate its handling of the personal information in its computer networks.

After answering the FTC's complaint, LabMD filed a motion to dismiss it for failure to state a case cognizable under Section 5. The motion essentially replicated the assertions in LabMD's answer. Under the FTC's Rules of Practice, the Commission, rather than the ALJ, ruled on the motion to dismiss. The Commission denied the motion, concluding that it had authority under Section 5(a) to prosecute the charge of unfairness asserted in its complaint. *LabMD, Inc.*, 2014-1 Trade Cases P 78784 (F.T.C.) (Jan. 16, 2014).

Following discovery, LabMD filed a motion for summary judgment, presenting arguments similar to those made in support of its motion to dismiss. As before, the motion was submitted to the Commission to decide. It denied the motion on the ground that there were genuine factual disputes relating to LabMD's liability "for engaging in unfair acts or practices in violation of Section 5(a)," necessitating an evidentiary hearing. *LabMD, Inc.*, 2014-1 Trade Cases P 78785

---

networks. As a result, respondent did not detect the installation or use of an unauthorized file sharing application on its networks.

(F.T.C.), at *1 (May 19, 2014) (quotations omitted). An evidentiary hearing was held before the ALJ in July 2015.[9]

After considering the parties' submissions, the ALJ dismissed the FTC's complaint, concluding that the FTC failed to prove that LabMD had committed unfair acts or practices in neglecting to provide adequate security for the personal information lodged in its computer networks. Namely, the FTC failed to prove that LabMD's "alleged failure to employ reasonable data security . . . caused or is likely to cause substantial injury to consumers," as required by Section 5(n) of the Act, 15 U.S.C. § 45(n).[10] Because there was no substantial injury or likelihood thereof, there could be no unfair act or practice.

The FTC appealed the ALJ's decision, which under 16 C.F.R. § 3.52 brought the decision before the full Commission for review. In July 2016, reviewing the ALJ's findings of fact and conclusions of law *de novo*, *see id.* § 3.54, the FTC reversed the ALJ's decision.

The FTC first found that LabMD "failed to implement reasonable security measures to protect the sensitive consumer information on its computer network." Therefore, LabMD's "data security practices were unfair under Section 5." In

[9] Prior to the hearing, LabMD amended its answer and once again unsuccessfully moved to dismiss the FTC's complaint. Nothing in the answer or the motion is pertinent here.

[10] Section 5(n) states, as a prerequisite for an act or practice to be unfair, "[T]he act or practice [1] causes or is likely to cause substantial injury to consumers [2] which is not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition."

particular, LabMD failed to adequately secure its computer network, employ suitable risk-assessment tools, provide data-security training to its employees, and adequately restrict and monitor the computer practices of those using its network. Because of these deficiencies, the Commission continued, LimeWire was able to be installed on the LabMD billing manager's computer, and Tiversa was ultimately able to download the 1718 File. The Commission then held that, contrary to the ALJ's decision, the evidence showed that Section 5(n)'s "substantial injury" prong was met in two ways: the unauthorized disclosure of the 1718 File itself caused intangible privacy harm, and the mere exposure of the 1718 File on LimeWire was likely to cause substantial injury. The FTC went on to conclude that Section 5(n)'s other requirements were also met.[11]

Next, the Commission addressed and rejected LabMD's arguments that Section 5(a)'s "unfairness" standard—which, according to the Commission, is a reasonableness standard—is void for vagueness and that the Commission failed to provide fair notice of what data-security practices were adequate under Section 5(a). The FTC then entered an order vacating the ALJ's decision and enjoining LabMD to install a data-security program that comported with the FTC's standard of reasonableness. *See generally Appendix*. The order is to terminate on either July 28, 2036, or twenty years "from the most recent date that the [FTC] files a

[11] *See supra* note 10.

complaint . . . in federal court alleging any violation of the order, whichever comes later." *Id.* at 6.

C.

LabMD petitioned this Court to review the FTC's decision. LabMD then moved to stay enforcement of the FTC's cease and desist order pending review, arguing that compliance with the order was unfeasible given LabMD's defunct status and *de minimis* assets. After an FTC response urging against the stay, we granted LabMD's motion. *LabMD, Inc. v. FTC*, 678 F. App'x 816 (11th Cir. 2016).

II.

Now, LabMD argues that the Commission's cease and desist order is unenforceable because the order does not direct it to cease committing an unfair "act or practice" within the meaning of Section 5(a).[12] We review the FTC's legal conclusions *de novo* but give "some deference to [its] informed judgment that a particular commercial practice is to be condemned as 'unfair.'" *FTC v. Ind. Fed'n of Dentists*, 476 U.S. 447, 454, 106 S. Ct. 2009, 2016 (1986). We review the FTC's findings of facts under the "substantial evidence" standard, *McWane, Inc. v. FTC*, 783 F.3d 814, 824 (11th Cir. 2015), which requires "more than a mere

[12] LabMD's brief asserts several grounds for setting aside the FTC's order. The only issue we address is the enforceability of the FTC's order.

scintilla" of evidence "but less than a preponderance," *Dyer v. Barnhart*, 395 F.3d 1206, 1210 (11th Cir. 2005).

A.

Section 5(a) of the FTC Act authorizes the FTC to protect consumers by "prevent[ing] persons, partnerships, or corporations . . . from using unfair . . . acts or practices in or affecting commerce." The Act does not define the term "unfair." The provision's history, however, elucidates the term's meaning.

The FTC Act, passed in 1914, created the FTC and gave it power to prohibit "unfair methods of competition."[13] Rather than list "the particular practices to which [unfairness] was intended to apply," Congress "intentionally left development of the term 'unfair' to the Commission" through case-by-case litigation[14]—though, at the time of the FTC Act's inception, the FTC's primary mission was understood to be the enforcement of antitrust law.[15] In 1938, the Act was amended to provide that the FTC had authority to prohibit "unfair . . . acts or practices."[16] This amendment sought to clarify that the FTC's authority applied

[13] *See* Marc Winerman, *The Origins of the FTC: Concentration, Cooperation, Control, and Competition*, 71 Antitrust L.J. 1, 2–6 (2003).

[14] *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239–40, 92 S. Ct. 898, 903 (1972); *Atl. Ref. Co. v. FTC*, 381 U.S. 357, 367, 85 S. Ct. 1498, 1505 (1965); *see* S. Rep. No. 63-597, at 13 (1914); H.R. Rep. No. 63-1142, at 19 (1914).

[15] *See generally* Winerman, *supra* note 13.

[16] *Id.* at 96.

not only to competitors but, importantly, also to consumers.[17] Hence, the FTC possesses "unfairness authority" to prohibit and prosecute unfair acts or practices harmful to consumers.

In 1964, the FTC set forth three factors to consider in deciding whether to wield its unfairness authority. The FTC was to consider whether an act or practice (1) caused consumers, competitors, or other businesses substantial injury; (2) offended public policy as established by statute, the common law, or otherwise; and (3) was immoral, unethical, or unscrupulous.[18] The Supreme Court cited these factors with apparent approval in dicta in the 1972 case *FTC v. Sperry & Hutchinson*, 405 U.S. 233, 244 n.5, 92 S. Ct. 898, 905 n.5 (1972).

"Emboldened" by *Sperry & Hutchinson*'s dicta, "the Commission set forth to test the limits of the unfairness doctrine."[19] This effort peaked in a 1978 attempt to "use unfairness to ban all advertising directed to children on the grounds that it was 'immoral, unscrupulous, and unethical' and based on generalized public policies to protect children."[20] Congress and much of the public disapproved.[21]

---

[17] *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 384, 85 S. Ct. 1035, 1042 (1965); H.R. Rep. No. 75-1613, at 3 (1937).

[18] Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking, Statement of Basis and Purpose, 29 Fed. Reg. 8324, 8355 (July 2, 1964).

[19] J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, FTC (May 30, 2003), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection.

[20] *Id.*

Congressional backlash included refusing to fund the FTC, thus shutting it down for several days, and passing legislation that prevented the FTC from using its unfairness authority to promulgate rules that restrict children's advertising.[22]

Following this episode, the Commission wrote a unanimous letter to two senators in 1980[23] placing gloss on the three 1964 unfairness factors that were recognized in *Sperry & Hutchinson*. As to the first factor, consumer injury, the FTC laid out a separate three-part test defining a qualifying injury. These consumer-injury factors would later be codified in Section 5(n). The FTC stated that to warrant a finding of unfairness, an injury "[1] must be substantial; [2] it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and [3] it must be an injury that consumers themselves could not reasonably have avoided."

As to the second 1964 unfairness factor, public policy, the FTC specified that the policies relied upon "should be clear and well-established"—that is, "declared or embodied in formal sources such as statutes, judicial decisions, or the Constitution as interpreted by the courts, rather than being ascertained from the

---

[21] *See, e.g.*, *The FTC as National Nanny*, Wash. Post (Mar. 1, 1978), https://www.washingtonpost.com/archive/politics/1978/03/01/the-ftc-as-national-nanny/69f778f5-8407-4df0-b0e9-7f1f8e826b3b/?utm_term=.015de8e7203d.

[22] Beales, *supra* note 19 (citing FTC Improvements Act of 1980, Pub. L. No. 96-252, § 14, 94 Stat. 388); *see* 15 U.S.C. § 57a(h).

[23] *FTC Policy Statement on Unfairness*, FTC (Dec. 17, 1980), available at https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

general sense of the national values." Put another way, an act or practice's "unfairness" must be grounded in statute, judicial decisions—*i.e.*, the common law—or the Constitution. An act or practice that causes substantial injury but lacks such grounding is not unfair within Section 5(a)'s meaning.[24] Finally, the FTC stated that it was nixing the third 1964 unfairness factor—whether a practice is immoral, unethical, or unscrupulous—because it was "largely duplicative" of the first two. Thus, an "unfair" act or practice is one which meets the consumer-injury factors listed above and is grounded in well-established legal policy.

B.

Here, the FTC's complaint alleges that LimeWire was installed on the computer used by LabMD's billing manager. This installation was contrary to company policy.[25] The complaint then alleges that LimeWire's installation caused the 1718 File, which consisted of consumers' personal information, to be exposed. The 1718 File's exposure caused consumers injury by infringing upon their right of privacy. Thus, the complaint alleges that LimeWire was installed in defiance of

[24] Section 5(n) now states, with regard to public policy, "In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination." We do not take this ambiguous statement to mean that the Commission may bring suit purely on the basis of substantial consumer injury. The act or practice alleged to have caused the injury must still be unfair under a well-established legal standard, whether grounded in statute, the common law, or the Constitution.

[25] The FTC's complaint does not state that LimeWire was installed contrary to company policy. But the complaint implies as much in that it does not allege that LabMD's policy allowed the installation. Further, undisputed evidence in the record indicates that LimeWire was installed contrary to LabMD policy.

LabMD policy and caused the alleged consumer injury. Had the complaint stopped there, a narrowly drawn and easily enforceable order might have followed, commanding LabMD to eliminate the possibility that employees could install unauthorized programs on their computers.

But the complaint continues past this single allegation of wrongdoing, adding that LimeWire's installation was not the only conduct that caused the 1718 File to be exposed. It also alleges broadly that LabMD "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks." The complaint then provides a litany of security measures that LabMD failed to employ, each setting out in general terms a deficiency in LabMD's data-security protocol.[26] Because LabMD failed to employ these measures, the Commission's theory goes, LimeWire was able to be installed on the billing manager's computer. LabMD's policy forbidding employees from installing programs like LimeWire was insufficient.

The FTC's complaint, therefore, uses LimeWire's installation, and the 1718 File's exposure, as an entry point to broadly allege that LabMD's data-security operations are deficient as a whole. Aside from the installation of LimeWire on a company computer, the complaint alleges no specific unfair acts or practices engaged in by LabMD. Rather, it was LabMD's multiple, unspecified failures to

[26] *See supra* note 8.

act in creating and operating its data-security program that amounted to an unfair act or practice.[27] Given the breadth of these failures, the Commission attached to its complaint a proposed order which would regulate all aspects of LabMD's data-security program—sweeping prophylactic measures to collectively reduce the possibility of employees installing unauthorized programs on their computers and thus exposing consumer information. The proposed cease and desist order, which is identical in all relevant respects to the order the FTC ultimately issued, identifies no specific unfair acts or practices from which LabMD must abstain and instead requires LabMD to implement and maintain a data-security program "reasonably designed" to the Commission's satisfaction. *See generally Appendix*.

---

[27] After outlining LabMD's shortcomings in data security, namely those items listed in note 8, *supra*, the FTC's complaint states in paragraph 22 that LabMD's

> failure to employ reasonable and appropriate measures to prevent unauthorized access to personal information, including dates of birth, SSNs, medical test codes, and health information, caused, or is likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. *This practice was, and is, an unfair act or practice*.

(Emphasis added). Oddly, paragraph 23 of the complaint states that the "*acts and practices* of [LabMD] as alleged in this complaint constitute unfair *acts or practices* in or affecting commerce in violation of Section 5(a)." (Emphasis added). Thus, paragraph 22 seems to conceive of all of LabMD's data-security deficiencies as culminating in a single unfair act or practice, and paragraph 23, though unspecific and perhaps boilerplate, suggests that there were multiple unfair acts or practices. Paragraph 22 better encapsulates the FTC's theory, as the complaint in preceding paragraphs lays out a number of deficiencies that, "taken together," constitute unreasonable data security. Further, the Commission's cease and desist order states, "[T]he Commission has concluded that LabMD's *data security practices were unreasonable* and *constitute an unfair act or practice* that violates Section 5." (Emphasis added). *See Appendix* at 1.

The decision on which the FTC based its final cease and desist order exhibits more of the same. The FTC found that LabMD "failed to implement reasonable security measures to protect the sensitive consumer information on its computer network" and that the failure caused substantial consumer injury. In effect, the decision held that LabMD's failure to act in various ways to protect consumer data rendered its entire data-security operation an unfair act or practice. The broad cease and desist order now at issue, according to the Commission, was therefore justified.

* * *

The first question LabMD's petition for review presents is whether LabMD's failure to implement and maintain a reasonably designed data-security program constituted an unfair act or practice within the ambit of Section 5(a). The FTC declared that it did because such failure caused substantial injury to consumers' right of privacy, and it issued a cease and desist order to avoid further injury.

The Commission must find the standards of unfairness it enforces in "clear and well-established" policies that are expressed in the Constitution, statutes, or the common law.[28] The Commission's decision in this case does not explicitly cite the source of the standard of unfairness it used in holding that LabMD's failure to

[28] *FTC Policy Statement on Unfairness*, *supra* note 23.

implement and maintain a reasonably designed data-security program constituted an unfair act or practice. It is apparent to us, though, that the source is the common law of negligence. According to the Restatement (Second) of Torts § 281 (Am. Law Inst. 1965), Statement of the Elements of a Cause of Action for Negligence,

> [an] actor is liable for an invasion of an interest of another, if:
>
> (a) the interest invaded is protected against unintentional invasion, and
>
> (b) the conduct of the actor is negligent with respect to the other, or a class of persons within which [the other] is included, and
>
> (c) the actor's conduct is a legal cause of the invasion, and
>
> (d) the other has not so conducted himself as to disable himself from bringing an action for such invasion.

The gist of the Commission's complaint and its decision is this: The consumers' right of privacy is protected against unintentional invasion. LabMD unintentionally invaded their right, and its deficient data-security program was a legal cause. Section 5(a) empowers the Commission to "prevent persons, partnerships, or corporations . . . from using unfair . . . acts or practices." The law of negligence, the Commission's action implies, is a source that provides standards for determining whether an act or practice is unfair, so a person, partnership, or corporation that negligently infringes a consumer interest protected against unintentional invasion may be held accountable under Section 5(a). We will assume *arguendo* that the Commission is correct and that LabMD's negligent

failure to design and maintain a reasonable data-security program invaded consumers' right of privacy and thus constituted an unfair act or practice.

The second question LabMD's petition for review presents is whether the Commission's cease and desist order, founded upon LabMD's general negligent failure to act, is enforceable. We answer this question in the negative. We illustrate why by first laying out the FTC Act's enforcement and remedial schemes and then by demonstrating the problems that enforcing the order would pose.

III.

The FTC carries out its Section 5(a) mission to prevent unfair acts or practices in two ways: formal rulemaking and case-by-case litigation.

The Commission is authorized under 15 U.S.C. § 57a to prescribe rules "which define with specificity" unfair acts or practices within the meaning of Section 5(a). Once a rule takes effect, it becomes in essence an addendum to Section 5(a)'s phrase "unfair . . . acts or practices"; the rule puts the public on notice that a particular act or practice is unfair. The FTC enforces its rules in the federal district courts. Under 15 U.S.C. § 45(m)(1)(A),[29] the Commission may

[29] This provision states,

> The Commission may commence a civil action to recover a civil penalty in a district court of the United States against any person, partnership, or corporation which violates any rule under this subchapter respecting unfair or deceptive acts or practices . . . with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by

bring an action to recover a civil penalty against any person, partnership or corporation that knowingly violates a rule.[30] This case does not involve the enforcement of an FTC-promulgated rule.

What is involved here is the FTC's establishment of an unfair act or practice through litigation. Because Congress thought impossible the task of legislating a comprehensive list of unfair acts or practices, it authorized the Commission to establish unfair acts or practices through case-by-case litigation. In the litigation context, once an act or practice is adjudged to be unfair, the act or practice becomes in effect—like an FTC-promulgated rule—an addendum to Section 5(a).

The FTC Act provides two forums for such litigation. The Commission may choose to prosecute its claim that an act or practice is unfair before an ALJ, with appellate review before the full Commission and then in a federal court of appeals. *See* 15 U.S.C. § 45(b), (c); 16 C.F.R. § 3.1 *et seq.* Or, under Section 13(b) of the Act, 15 U.S.C. § 53(b), it may prosecute its claim before a federal district judge, with appellate review also in a federal court of appeals.

---

> such rule. In such action, such person, partnership, or corporation shall be liable for a civil penalty of not more than $10,000 for each violation.

15 U.S.C. § 45(m)(1)(A). As explained in note 39, *infra*, the Commission has increased the penalty amount to $41,484 per violation.

[30] The Commission may also bring a suit in federal district court or a state court of competent jurisdiction to obtain relief in the form of consumer redress. 15 U.S.C. § 57b.

Assume a factual scenario in which the Commission believes a certain act or practice is unfair. It should not matter which of the two forums the Commission chooses to prosecute its claim. The result should be the same. As we explain below, the ALJ and the district judge use materially identical procedural rules in processing the case to judgment[31] and both apply the same substantive law to the facts. Further, putting any venue differences aside, the same court of appeals reviews their decisions.

A.

We consider the Commission's first option, litigation before an ALJ. The Commission issues an administrative complaint against a party it has reason to believe is engaging in an unfair act or practice and seeks a cease and desist order. 16 C.F.R. § 3.13. The Commission prosecutes the complaint before an ALJ whom it designates, in accordance with its Rules of Practice. *Id.* § 3.1 *et seq.* Under these Rules, the complaint must provide, among other things, "[a] clear and concise factual statement sufficient to inform each respondent with reasonable definiteness of the type of acts or practices alleged to be in violation of the law."

[31] *See* FTC, *Operating Manual* Chapter 10.7, available at https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch10administrativelitigation.pdf (stating that "many [of the Commission's] adjudicative rules are derived from the Federal Rules of Civil Procedure"); *see also* Stephanie W. Kanwit, *Federal Trade Commission* § 8:1 (2017) (noting that the Commission "has held over the years that the [Federal Rules of Civil Procedure] can provide an analytical framework for the disposition of related issues" (quotations omitted)).

*Id.* § 3.11. If the respondent files a motion to dismiss the complaint, the motion is referred to the Commission for a ruling.[32] If the motion is denied, the respondent files an answer. From that point on, the proceedings before the ALJ resemble the proceedings in an action for injunctive relief in federal district court. If the ALJ finds that the respondent has been engaging in the unfair act or practice alleged and will likely continue doing so, the ALJ enters a cease and desist order enjoining the respondent from engaging in the unfair conduct.[33] If not, the ALJ dismisses the Commission's complaint.[34] Either way, the ALJ's decision is appealable to the FTC, *id.* § 3.52, and the FTC's decision is in turn reviewable in a federal court of appeals, 15 U.S.C. § 45(c).

Suppose the Commission chooses the second option, litigation before a federal district judge under Section 13(b). If the Commission has reason to believe a party is engaging in an unfair act or practice, it seeks an injunction by filing in district court a complaint that sets forth "well-pleaded facts . . . permit[ting] the court to infer more than the mere possibility of misconduct." *Ashcroft v. Iqbal*, 556 U.S. 662, 679, 129 S. Ct. 1937, 1950 (2009) (citing Fed. R. Civ. P. 8(a)(2)).

---

[32] The Commission may, in its discretion, refer the motion back to the ALJ for a ruling. 16 C.F.R. § 3.22.

[33] The ALJ's decision must set out findings of fact and conclusions of law, 16 C.F.R. § 3.51(c), just like a district judge must do pursuant to Federal Rule of Civil Procedure 52(a) following a bench trial.

[34] As a whole, this administrative procedure, set out in the FTC's Rules of Practice, effectively supersedes 15 U.S.C. § 45(b), the FTC Act provision governing Commission proceedings.

Although the case is tried pursuant to the Federal Rules of Civil Procedure, not the FTC Rules of Practice, it is handled essentially as it would be before the ALJ. If the district judge finds that the defendant has been engaging in the unfair act or practice alleged and will likely continue doing so, the judge enjoins the defendant from engaging in such conduct. Whatever the court's decision, it is reviewable in the court of appeals.

Assume the result is the same in both litigation forums. The ALJ enters a cease and desist order; the district court issues an injunction. Appellate review would reach the same result regardless of the trial forum (assuming that venue is laid in the same court of appeals).[35] Assume further that both coercive orders are affirmed by the court of appeals. The cease and desist order and the injunction address the same behavior and contain the same command: discontinue engaging in a specific unfair act or practice.

---

[35] There are a couple of subtle differences in how cease and desist orders and injunctions are reviewed. First, an appellate court reviews a district court's findings of fact for clear error and those of the FTC under the "substantial evidence" standard. *McWane, Inc.*, 783 F.3d at 824; *Dyer*, 395 F.3d at 1210. In practice, however, these two standards make little or no difference in terms of outcome. *See Dickinson v. Zurko*, 527 U.S. 150, 162–63, 119 S. Ct. 1816, 1823 (1999) ("The court/agency [substantial-evidence] standard, as we have said, is somewhat less strict than the court/court [clearly erroneous] standard. But the difference is a subtle one—so fine that (apart from the present case) we have failed to uncover a single instance in which a reviewing court conceded that use of one standard rather than the other would in fact have produced a different outcome."). Further, although both the FTC's and a district court's conclusions of law are reviewed *de novo*, appellate courts give "some deference to the Commission's informed judgment that a particular commercial practice is to be condemned as 'unfair.'" *Ind. Fed'n of Dentists*, 476 U.S. at 454, 106 S. Ct. at 2016.

With the cease and desist order or the injunction in hand, the Commission may proceed in two ways against a party who violates its terms.[36] The Commission may seek the imposition of either a civil penalty or civil-contempt sanction.[37] We explain below the procedures the Commission invokes in pursuing these respective remedies.

B.

1.

Under Section 5(*l*), 15 U.S.C. § 45(*l*), the Commission may bring a civil-penalty action in district court should the respondent violate a final cease and desist order.[38] The Commission's complaint would allege that the defendant is subject to an existing cease and desist order and has violated its terms. For each separate

---

[36] We note that with respect to violations of final cease and desist orders, the Commission may also bring a 15 U.S.C. § 57b action as described in note 30, *supra*.

[37] The two remedies are similar in nature. Indeed, not long after Section 5's civil-penalty scheme was implemented, the Commissioner of the FTC described civil penalties as "an additional remedy to that formerly employed of invoking the inherent power of the courts to punish for contempt anyone who violated a court order directing compliance with an order of the Commission." *See* Hon. R. E. Freer, Commissioner, Federal Trade Commission, Address before the Annual Convention of the Proprietary Association (May 17, 1938).

[38] A cease and desist order is made final pursuant to the conditions set forth in 15 U.S.C. § 45(g). Section 5(*l*) directs the Commission to call upon the United States Attorney General to commence a civil-penalty action against the respondent. The Commission can bring the action itself, however, in accordance with the criteria in 15 U.S.C. § 56(a).

Section 5(m)(1)(B) of the Act, 15 U.S.C. § 45(m)(1)(B), authorizes the Commission to file suit against a nonrespondent who "with actual knowledge" engages in the "act or practice" declared a violation of Section 5(a) and enjoined via a cease and desist order entered in a previous administrative adjudication. The previous adjudication, however, is afforded no collateral estoppel effect against the defendant. That is, the defendant can challenge the factual predicate for the cease and desist order and the ultimate determination that the facts found in the previous adjudication constituted an unfair act or practice. *See id.* § 45(m)(2).

violation of the order—or, in the case of a continuing violation, for each day in violation—the district court may impose a penalty of up to $41,484.[39] *Id.* Section 5(*l*) also empowers the district court to grant an injunction if the Commission proves that the violation is likely to continue and an injunction is necessary to enforce the order.

If the Commission has obtained an injunction in district court requiring the defendant to discontinue an unfair act or practice, it may invoke the district court's civil-contempt power should the defendant disobey. Rather than filing a complaint, as in a Section 5(*l*) action, the Commission simply moves the district court for an order requiring the defendant to show cause why it should not be held in contempt for engaging in conduct the injunction specifically enjoined. If the court is satisfied that the conduct is forbidden, it issues a show cause order. Then, if at the show cause hearing the Commission establishes by clear and convincing proof that the defendant engaged in the forbidden conduct and that the defendant "had the ability to comply" with the injunctive provision at issue, *McGregor v. Chierico*, 206 F.3d 1378, 1383 (11th Cir. 2000), the court may adjudicate the defendant in civil contempt and impose appropriate sanctions.

---

[39] Sections 5(*l*) and 5(m)(1)(B) set the maximum penalty at $10,000, but the Commission may adjust this figure for inflation under 16 C.F.R. § 1.98. Hence the current $41,484 figure, which "appl[ies] only to penalties assessed after January 22, 2018" but "includ[es] those penalties whose associated violation predated January 22, 2018." *Id.*

2.

The concept of specificity is crucial to both modes of enforcement. We start with civil penalties for violations of cease and desist orders. Nothing in the FTC Act addresses what content must go into a cease and desist order. The FTC Rule of Practice governing Commission complaints, however, states that a complaint must contain "[a] clear and concise factual statement sufficient to inform each respondent with reasonable definiteness of the type of acts or practices alleged to be in violation of the law." 16 C.F.R § 3.11. It follows that the remedy the complaint seeks must comport with this requirement of reasonable definiteness. Moreover, given the severity of the civil penalties a district court may impose for the violation of a cease and desist order, the order's prohibitions must be stated with clarity and precision. The United States Supreme Court emphasized this point in *FTC v. Colgate-Palmolive Co.*, stating,

> [T]his Court has . . . warned that an order's prohibitions should be clear and precise in order that they may be understood by those against whom they are directed, and that [t]he severity of possible penalties prescribed . . . for violations of orders which have become final underlines the necessity for fashioning orders which are, at the outset, sufficiently clear and precise to avoid raising serious questions as to their meaning and application.

380 U.S. 374, 392, 85 S. Ct. 1035, 1046 (1965) (quotations and citations omitted). The imposition of penalties upon a party for violating an imprecise cease and desist

order—up to $41,484 per violation or day in violation—may constitute a denial of due process.[40]

Specificity is equally important in the fashioning and enforcement of an injunction consequent to an action brought in district court under Section 13(b). Federal Rule of Civil Procedure 65(d)(1) requires that an injunctive order state the reasons for its coercive provisions, state the provisions "specifically," and describe the acts restrained or required "in reasonable detail." The Supreme Court has stated that Rule 65(d)(1)'s "specificity provisions . . . are no mere technical requirements. The Rule was designed to prevent uncertainty and confusion on the part of those faced with injunctive orders, and to avoid the possible founding of a contempt citation on a decree too vague to be understood." *Schmidt v. Lessard*, 414 U.S. 473, 476, 94 S. Ct. 713, 715 (1974). Indeed, "[t]he most fundamental postulates of our legal order forbid the imposition of a penalty for disobeying a command that defies comprehension." *Int'l Longshoremen's Ass'n, Local 1291 v. Phila. Marine Trade Ass'n*, 389 U.S. 64, 76, 88 S. Ct. 201, 208 (1967). Being held in contempt and sanctioned pursuant to an insufficiently specific injunction is

---

[40] *See BMW of N. Am., Inc. v. Gore*, 517 U.S. 559, 574 & n.22, 116 S. Ct. 1589, 1598 & n.22 (1996) ("Elementary notions of fairness enshrined in our constitutional jurisprudence dictate that a person receive fair notice . . . of the conduct that will subject him to punishment . . . . [T]he basic protection against judgments without notice afforded by the Due Process Clause is implicated by civil penalties." (citation, quotations, and emphasis omitted)); *see also Sessions v. Dimaya*, 584 U.S. —, 138 S. Ct. 1204, 1228–29 (2018) (Gorsuch, J., concurring) (suggesting that the severity of a civil penalty corresponds with the degree of fair notice of unlawful conduct that must be accorded to the defendant).

therefore a denial of due process. *See id.* (reversing a civil-contempt judgment founded upon an order too vague to be understood).

In sum, the prohibitions contained in cease and desist orders and injunctions must be specific. Otherwise, they may be unenforceable. Both coercive orders are also governed by the same standard of specificity, as the stakes involved for a violation are the same—severe penalties or sanctions.

C.

In the case at hand, the cease and desist order contains no prohibitions. It does not instruct LabMD to stop committing a specific act or practice. Rather, it commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness. This command is unenforceable. Its unenforceability is made clear if we imagine what would take place if the Commission sought the order's enforcement. As we have explained, the standards a district court would apply are essentially the same whether it is entertaining the Commission's action for the imposition of a penalty or the Commission's motion for an order requiring the enjoined defendant to show cause why it should not be adjudicated in contempt. For ease of discussion, we posit a scenario in which the Commission obtained the coercive order it entered in this case from a district court, and now seeks to enforce the order.

The Commission moves the district court for an order requiring LabMD to show cause why it should not be held in contempt for violating the following injunctive provision:

> [T]he respondent shall . . . establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers . . . . Such program . . . shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers . . . .[41]

*See Appendix* at 2. The Commission's motion alleges that LabMD's program failed to implement "*x*" and is therefore not "reasonably designed." The court concludes that the Commission's alleged failure is within the provision's language and orders LabMD to show cause why it should not be held in contempt.

At the show cause hearing, LabMD calls an expert who testifies that the data-security program LabMD implemented complies with the injunctive provision at issue. The expert testifies that "*x*" is not a necessary component of a reasonably designed data-security program. The Commission, in response, calls an expert who disagrees. At this point, the district court undertakes to determine which of the two equally qualified experts correctly read the injunctive provision. Nothing in the provision, however, indicates which expert is correct. The provision

[41] Following this provision in the Commission's cease and desist order are five equally vague items which must be included in LabMD's data-security program. *See Appendix* at 2–3. These items suffer the same enforceability problems discussed below.

contains no mention of "*x*" and is devoid of any meaningful standard informing the court of what constitutes a "reasonably designed" data-security program.[42] The court therefore has no choice but to conclude that the Commission has not proven—and indeed cannot prove—LabMD's alleged violation by clear and convincing evidence. *See McGregor*, 206 F.3d at 1383.[43]

If the court held otherwise and ordered LabMD to implement "*x*," the court would have effectively modified the injunction at a show cause hearing. This would open the door to future modifications, all improperly made at show cause hearings.[44] Pretend that LabMD implemented "*x*" pursuant to the court's order, but the FTC, which is continually monitoring LabMD's compliance with the court's injunction, finds that "*x*" failed to bring the system up to the FTC's conception of reasonableness. So, the FTC again moves the district court for an order to show cause. This time, its motion alleges that LabMD failed to implement "*y*," another item the Commission thinks necessary to any reasonable data-security program.

---

[42] Further, the order's other provisions, mentioned in note 41, *supra*, also fail to state with specificity the actions LabMD must take to bring its program into compliance with the order.

[43] *See also FTC v. Trudeau*, 579 F.3d 754, 763 (7th Cir. 2009) ("To succeed on a contempt petition, the FTC must demonstrate by clear and convincing evidence that the respondent has violated the express and unequivocal command of a court order." (quotations omitted)).

[44] The purpose of a show cause hearing is to determine whether the alleged contemner has violated the injunctive provision as it stands. If the party holding the injunction wishes to modify the provision, the party must move the district court to effect the modification. Implicit in Federal Rule of Civil Procedure 65 is the notion that before the modification can be made, the adverse party must be provided notice of the proposed modification and an opportunity to be heard.

Does the court side with the Commission, modify the injunction, and order the implementation of "*y*"? Suppose "*y*" fails. Does another show cause hearing result in a third modification requiring the implementation of "*z*"?

The practical effect of repeatedly modifying the injunction at show cause hearings is that the district court is put in the position of managing LabMD's business in accordance with the Commission's wishes. It would be as if the Commission was LabMD's chief executive officer and the court was its operating officer. It is self-evident that this micromanaging is beyond the scope of court oversight contemplated by injunction law.

This all serves to show that an injunction identical to the FTC cease and desist order at issue would be unenforceable under a district court's contempt power. Because the standards governing the coercive enforcement of injunctions and cease and desist orders are the same, it follows that the Commission's cease and desist order is itself unenforceable.

IV.

In sum, assuming *arguendo* that LabMD's negligent failure to implement and maintain a reasonable data-security program constituted an unfair act or practice under Section 5(a), the Commission's cease and desist order is nonetheless unenforceable. It does not enjoin a specific act or practice. Instead, it mandates a complete overhaul of LabMD's data-security program and says precious little

about how this is to be accomplished. Moreover, it effectually charges the district court with managing the overhaul. This is a scheme Congress could not have envisioned. We therefore grant LabMD's petition for review and vacate the Commission's order.

**SO ORDERED.**

**UNITED STATES OF AMERICA**
**BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:** **Edith Ramirez, Chairwoman**
**Maureen K. Ohlhausen**
**Terrell McSweeny**

| | | |
|---|---|---|
| **In the Matter of** | ) | |
| | ) | **DOCKET NO. 9357** |
| **LabMD, Inc.,** | ) | |
| **a corporation.** | ) | **PUBLIC** |

# FINAL ORDER

The Commission has heard this matter upon the appeal of Complaint Counsel from the Initial Decision of the Administrative Law Judge, and upon briefs and oral argument in support thereof and in opposition thereto. For the reasons stated in the accompanying opinion of the Commission, the Commission has concluded that LabMD's data security practices were unreasonable and constitute an unfair act or practice that violates Section 5 of the Federal Trade Commission Act. The Commission has therefore determined to vacate the Initial Decision and issue the following order:

## ORDER

## DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

2. Unless otherwise specified, "respondent" shall mean LabMD, Inc., and its successors and assigns.

3. "Affected Individual" shall mean any consumer whose personal information LabMD has reason to believe was, or could have been, accessible to unauthorized persons before July 28, 2016, including, but not limited to, consumers listed in the Insurance File and other documents available to a peer-to-peer file sharing network, but excluding consumers whom LabMD has notified, before July 28, 2016, of a data security breach.

4. "Insurance File" shall mean the file containing personal information about approximately 9,300 consumers, including names, dates of birth, Social Security numbers, health insurance company names and policy numbers, and medical test codes, that was available to a peer-to-peer file sharing network through a peer-to-peer file sharing application installed on a computer on respondent's computer network.

5. "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number.

**I.**

**IT IS ORDERED** that the respondent shall, no later than the date this order becomes final and effective, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers by respondent or by any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program;

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and

E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by Subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

**II.**

**IT IS FURTHER ORDERED** that, in connection with its compliance with Part I of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after July 28, 2016, for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after July 28, 2016, for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by Part I of this order; and

D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected, and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not

the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC Docket No. 9357. Provided, however, that in lieu of overnight courier, Assessments may be sent by first-class mail, but only if an electronic version of any such Assessment is contemporaneously sent to the Commission at Debrief@ftc.gov.

**III.**

**IT IS FURTHER ORDERED** that respondent shall provide notice to Affected Individuals and their health insurance companies within 60 days of the date this order becomes final and effective unless an appropriate notice has already been provided, as follows:

A. Respondent shall send the notice to each Affected Individual by first class mail, only after obtaining acknowledgment from the Commission or its staff that the form and substance of the notice satisfies the provisions of the order. The notice must be easy to understand and must include:

1. a brief description of why the notice is being sent, including the approximate time period of the unauthorized disclosure, the types of personal information that were or may have been disclosed without authorization (*e.g.*, insurance information, Social Security numbers, etc.), and the steps respondent has taken to investigate the unauthorized disclosure and protect against future unauthorized disclosures;

2. advice on how Affected Individuals can protect themselves from identity theft or related harms. Respondent may refer Affected Individuals to the Commission's identity theft website (www.ftc.gov/idtheft), advise them to contact their health care providers or insurance companies if bills don't arrive on time or contain irregularities, or to obtain a free copy of their credit report from www.annualcreditreport.com and monitor it and their accounts for suspicious activity, or take such other steps as respondent deems appropriate; and

3. methods by which Affected Individuals can contact respondent for more information, including a toll-free number for 90 days after notice to Affected Individuals, an email address, a website, and mailing address.

B. Respondent shall send a copy of the notice to each Affected Individual's health insurance company by first class mail.

C. If respondent does not have an Affected Individual's mailing address in its possession, it shall make reasonable efforts to find such mailing address, such as by reviewing online directories, and once found, shall provide the notice described in Subpart A, above.

**IV.**

**IT IS FURTHER ORDERED** that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including, but not limited to, notice letters required by Part III of this order and documents, prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and

B. for a period of three (3) years after the date of preparation of each Assessment required under Part II of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts I and II of this order, for the compliance period covered by such Assessment.

**V.**

**IT IS FURTHER ORDERED** that respondent shall deliver a copy of this order to: (1) all current and future principals, officers, directors, and managers; (2) all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order; and (3) any business entity resulting from any change in structure set forth in Part VI. Respondent shall deliver this order to such current personnel within thirty (30) days after the date this order becomes final and effective, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure.

**VI.**

**IT IS FURTHER ORDERED** that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC Docket No. 9357. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

**VII.**

**IT IS FURTHER ORDERED** that respondent, within sixty (60) days after the date this order becomes final and effective, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, they shall submit additional true and accurate written reports. Unless otherwise directed by a representative of the Commission in writing, all notices required by this Part shall be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC Docket No. 9357. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

**VIII.**

This order will terminate on July 28, 2036, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in less than twenty (20) years;

B. this order's application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that each respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: July 28, 2016