1023099

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	
LabMD, Inc.,	)	**DOCKET NO. 9357**
a corporation.	)	
	)	**PROVISIONALLY REDACTED**
	)	**PUBLIC VERSION**

COMPLAINT

The Federal Trade Commission ("Commission"), having reason to believe that LabMD, Inc. ("LabMD" or "respondent"), a corporation, has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

RESPONDENT'S BUSINESS

1. Respondent LabMD is a Georgia corporation with its principal office or place of business at 2030 Powers Ferry Road, Building 500, Suite 520, Atlanta, Georgia 30339.

2. The acts and practices of respondent alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

3. Since at least 2001, respondent has been in the business of conducting clinical laboratory tests on specimen samples from consumers and reporting test results to consumers' health care providers.

4. Respondent files insurance claims for charges related to the clinical laboratory tests with health insurance companies. Insured consumers typically pay the part of respondent's charges not covered by insurance; uninsured consumers are responsible for the full amount of the charges. Consumers in many instances pay respondent's charges with credit cards or personal checks.

5. Respondent tests samples from consumers located throughout the United States.

6. In performing tests, respondent routinely obtains information about consumers, including, but not limited to: names; addresses; dates of birth; gender; telephone numbers; Social Security numbers ("SSN"); medical record numbers; bank account or credit card information; health care provider names, addresses, and telephone numbers; laboratory tests, test codes and results, and diagnoses; clinical histories; and health insurance company names and policy numbers (collectively, "personal information").

7. Respondent has accumulated and maintains personal information for nearly one million consumers.

8. Respondent operates computer networks in conducting its business. The computer networks include computers, servers, and other devices in respondent's corporate offices and laboratory, computers used by its personnel in different parts of the country, and computers that respondent provides to some health care providers.

9. Among other things, respondent uses the computer networks to: receive orders for tests from health care providers; report test results to health care providers; file insurance claims with health insurance companies; prepare bills and other correspondence to consumers; obtain approvals for payments made by consumers with credit cards; and prepare medical records. For example, respondent's billing department uses the computer networks to generate or access documents related to processing claims and payments, such as:

   (a) monthly spreadsheets of insurance claims and payments ("insurance aging reports"), which may include personal information such as consumer names, dates of birth, SSNs, the American Medical Association current procedural terminology ("CPT") codes for the laboratory test conducted, and health insurance company names, addresses, and policy numbers;

   (b) spreadsheets of payments received from consumers ("Day Sheets"), which may include personal information such as consumer names, SSNs, and methods, amounts, and dates of payments; and

   (c) copies of consumer checks, which may include personal information such as names, addresses, telephone numbers, payment amounts, bank names and routing numbers, and bank account numbers ("copied checks").

RESPONDENT'S SECURITY PRACTICES

10. At all relevant times, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks. Among other things, respondent:

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

11. Respondent could have corrected its security failures at relatively low cost using readily available security measures.

12. Consumers have no way of independently knowing about respondent's security failures and could not reasonably avoid possible harms from such failures, including identity theft, medical identity theft, and other harms, such as disclosure of sensitive, private medical information.

PEER-TO-PEER FILE SHARING APPLICATIONS

13. Peer-to-peer ("P2P") file sharing applications are often used to share music, videos, pictures, and other materials between persons and entities using computers with the same or a compatible P2P application ("P2P network").

14. P2P applications allow a user to both designate files on the user's computer that are available to others on a P2P network and search for and access designated files on other computers on the P2P network.

15. After a designated file is shared with another computer, it can be passed along among other P2P network users without being downloaded again from the original source. Generally, once shared, a file cannot with certainty be removed permanently from a P2P network.

16. Since at least 2005, security professionals and others (including the Commission) have warned that P2P applications present a risk that users will inadvertently share files on P2P networks.

SECURITY INCIDENTS

17. In May 2008, a third party informed respondent that its June 2007 insurance aging report (the "P2P insurance aging file") was available on a P2P network through Limewire, a P2P file sharing application.

18. After receiving the May 2008 notice that the P2P insurance aging file was available through Limewire, respondent determined that:

    (a) Limewire had been downloaded and installed on a computer used by respondent's billing department manager (the "billing computer");

    (b) at that point in time, the P2P insurance aging file was one of hundreds of files that were designated for sharing from the billing computer using Limewire; and

    (c) Limewire had been installed on the billing computer no later than 2006.

19. The P2P insurance aging file contains personal information about approximately 9,300 consumers, including names, dates of birth, SSNs, CPT codes, and, in many instances, health insurance company names, addresses, and policy numbers.

20. Respondent had no business need for Limewire and removed it from the billing computer in May 2008, after receiving notice.

21. In October 2012, the Sacramento, California Police Department found more than 35 Day Sheets and a small number of copied checks in the possession of individuals who pleaded no contest to state charges of identity theft. These Day Sheets include personal information, such as names and SSNs, of several hundred consumers in different states. Many of these consumers were not included in the P2P insurance aging file, and some of the information post-dates the P2P insurance aging file. A number of the SSNs in the Day Sheets are being, or have been, used by people with different names, which may indicate that the SSNs have been used by identity thieves.

VIOLATION OF THE FTC ACT

22. As set forth in Paragraphs 6 through 21, respondent'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.

23. The acts and practices of respondent as alleged in this complaint constitute unfair acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C § 45(a).

NOTICE

Notice is hereby given to the respondent that the twenty-eighth day of April, 2014, at 10:00 a.m., is hereby fixed as the time, and the Federal Trade Commission offices at 600 Pennsylvania Avenue, N.W., Room 532-H, Washington, D.C. 20580, as the place when and where a hearing will be had before an Administrative Law Judge of the Federal Trade Commission, on the charges set forth in this complaint, at which time and place you will have the right under the Federal Trade Commission Act to appear and show cause why an order should not be entered requiring you to cease and desist from the violations of law charged in this complaint.

You are notified that the opportunity is afforded you to file with the Federal Trade Commission an answer to this complaint on or before the fourteenth (14th) day after service of it upon you. An answer in which the allegations of the complaint are contested shall contain a concise statement of the facts constituting each ground of defense; and specific admission, denial, or explanation of each fact alleged in the complaint or, if you are without knowledge thereof, a statement to that effect. Allegations of the complaint not thus answered shall be deemed to have been admitted.

If you elect not to contest the allegations of fact set forth in the complaint, the answer shall consist of a statement that you admit all of the material facts to be true. Such an answer shall constitute a waiver of hearings as to the facts alleged in the complaint and, together with the complaint, will provide a record basis on which the Commission shall issue a final decision containing appropriate findings and conclusions, and a final order disposing of the proceeding. In such answer, you may, however, reserve the right to submit proposed findings of fact and conclusions of law under Rule 3.46 of the Commission's Rules of Practice for Adjudicative Proceedings.

Failure to answer within the time above provided shall be deemed to constitute a waiver of your right to appear and to contest the allegations of the complaint, and shall authorize the Commission, without further notice to you, to find the facts to be as alleged in the complaint and to enter a final decision containing appropriate findings and conclusions and a final order disposing of the proceeding.

The Administrative Law Judge shall hold a prehearing scheduling conference not later than ten (10) days after the answer is filed by the respondent. Unless otherwise directed by the Administrative Law Judge, the scheduling conference and further proceedings will take place at the Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Room 532-H, Washington, D.C. 20580. Rule 3.21(a) requires a meeting of the parties' counsel as early as practicable before the prehearing scheduling conference, but in any event no later than five (5) days after the answer is filed by the respondent. Rule 3.31(b) obligates counsel for each party, within five (5) days of receiving respondent's answer, to make certain disclosures without awaiting a formal discovery request.

The following is the form of order which the Commission has reason to believe should issue if the facts are found to be as alleged in the complaint. If, however, the Commission should conclude from record facts developed in any adjudicative proceedings in this matter that the proposed order provisions might be inadequate to fully protect the consuming public, the Commission may order such other relief as it finds necessary or appropriate.

Moreover, the Commission has reason to believe that, if the facts are found as alleged in the complaint, it may be necessary and appropriate for the Commission to seek relief to redress injury to consumers, or other persons, partnerships or corporations, in the form of restitution for past, present, and future consumers and such other types of relief as are set forth in Section 19(b) of the Federal Trade Commission Act. The Commission will determine whether to apply to a court for such relief on the basis of the adjudicative proceedings in this matter and such other factors as are relevant to consider the necessity and appropriateness of such action.

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 the date of service of this order, including, but not limited to, consumers listed in the Insurance File and the Sacramento Documents.

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.

6. "Sacramento Documents" shall mean the documents identified in Appendix A.

I.

IT IS ORDERED that the respondent shall, no later than the date of service of this order, 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 service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order 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 the 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 File No.1023099. 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 service of this order 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 service of this order, 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 File No. 1023099. 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 of service of this order, 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 File No. 1023099.

VIII.

This order will terminate twenty (20) years from the date of its issuance, 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.

IN WITNESS WHEREOF, the Federal Trade Commission has caused this complaint to be signed by its Secretary and its official seal to be hereto affixed, at Washington, D.C. this twenty-eighth day of August, 2013.

By the Commission.

Donald S. Clark
Secretary