

UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION  
OFFICE OF ADMINISTRATIVE LAW JUDGES

_____ )	DOCKET NO. 9357
In the Matter of )	
)	PUBLIC
LabMD, Inc., )	
a corporation. )	ORAL ARGUMENT
_____ )	REQUESTED

**RESPONDENT LABMD, INC.'S MOTION FOR A PROTECTIVE ORDER**

Pursuant to Federal Trade Commission Rule 3.31(d), 16 C.F.R. § 3.31(d), Respondent LabMD, Inc. hereby moves the Administrative Law Judge for a protective order. This motion is supported by the attached exhibits and accompanying memorandum. Respondent respectfully requests a hearing on all issues raised in this motion.

Respectfully submitted,



Reed D. Rubinstein, Esq.  
William Sherman, II, Esq.  
Dinsmore & Shohl, L.L.P.  
801 Pennsylvania Ave., NW, Suite 610  
Washington, D.C. 20006  
Telephone: 202.372.9120  
Fax: 202.372.9141  
Email: reed.rubinstein@dinsmore.com



Michael D. Pepson *per telephone authorization*  
Cause of Action  
1919 Pennsylvania Ave., NW, Suite 650  
Washington, D.C. 20006  
Phone: 202.499.4232  
Email: michael.pepson@causeofaction.org  
Admitted only in Maryland.  
Practice limited to cases in federal court and  
administrative proceedings before federal agencies.

Dated: November 5, 2013

UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION  
OFFICE OF THE ADMINISTRATIVE LAW JUDGES

	)		
In the Matter of	)		DOCKET NO. 9357
	)		
LabMD, Inc.,	)		PUBLIC
a corporation.	)		ORAL ARGUMENT
	)		REQUESTED

**RESPONDENT LABMD, INC.’S MEMORANDUM IN SUPPORT OF MOTION FOR A PROTECTIVE ORDER**

Petitioner LabMD, Inc. (“LabMD”) hereby moves the Administrative Law Judge, under 16 C.F.R. § 3.31(d), to issue a protective order limiting or barring the more than twenty (20) third-party subpoenas for testimony and more than fifteen (15) third-party subpoenas for documents issued to LabMD’s current and former employees, clients, and IT service providers.<sup>1</sup>

**FACTS**

LabMD provides doctors with cancer-detection services. Its patient-information data-security practices are regulated by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and the Health Information Technology for Economic and Clinical Health Act (“HITECH”). LabMD has not violated these laws.

---

<sup>1</sup> This motion concerns the subpoenas issued to Allen Truett, 21<sup>st</sup> Century Oncology, Alison Simmons, Automated PC Technologies, David Lapides, Cyprus Communications, Eric Knox, Erick Garcia, Jeff Martin, Forensic Strategy Services, Karalyn Garrett, Josie Maldonado, John Boyle, Karina Jestes, Lawrence Hudson, Jeremy Dooley, Managed Data Solutions, Matt Bureau, MasterCard Worldwide, Patrick Howard, ProviDyn, Robert Hyer, Rosalind Woodson, Sacramento Police Dept., Sandy Springs GA Police Depart., Scott Moulton, Trend Micro, Inc., US Bank Nat’l Ass’n, Chris Maire, Visa Inc., Michael Daugherty, and Southeast Urology Network. The subpoenas are attached as Exhibit 1. The FTC has *already* deposed Mr. Daugherty and Mr. Boyle.

FTC notified LabMD on January 19, 2010, of a “non-public inquiry into LabMD, Inc.’s, compliance with federal law governing information security” because an internet security company called Tiversa Holding Corp. (“Tiversa”) had illicitly taken a LabMD patient information file (“PI file”) and given it to FTC after LabMD had turned down Tiversa’s new business pitch. FTC did not specify the regulations LabMD violated because FTC had not promulgated any.

On February 24, 2010, LabMD produced over 5,000 pages of documents. More were sent on June 4 and again on July 16. On July 23, LabMD’s principals were examined by the FTC counsel. On August 30, LabMD produced another 925 pages. On February 23, 2011, the FTC demanded more, and LabMD complied on May 16 and May 31. On December 11, the FTC issued formal civil investigative demands (the “CIDs”). LabMD petitioned to quash. Commissioner Brill denied this and LabMD appealed. Three Commissioners affirmed Commissioner Brill’s ruling, but Commissioner Rosch dissented, saying:

Tiversa...has a financial interest in intentionally exposing and capturing sensitive files on computer networks,...Tiversa used its robust, patented peer-to-peer monitoring technology to retrieve [LabMD’s file], and then repeatedly solicited LabMD...long before Commission staff contacted LabMD. In my view...the Commission should avoid even the appearance of bias or impropriety by not relying on such evidence or information in this investigation.

FTC petitioned for an order in the U.S. District Court for the Northern District of Georgia. The Court said that “there is significant merit to...[LabMD’s] argument that Section 5 does not justify an investigation into data security practices and consumer privacy issues....”<sup>2</sup>

---

<sup>2</sup> *FTC v. LabMD*, Case No. 1:12-cv-3005-WSD, at \*6-7 (N.D. Ga. Nov. 26, 2012).

But it upheld the CIDs, leaving LabMD to endure two more investigative hearings,<sup>3</sup> producing yet more documents.

On August 28, 2013, FTC issued a Complaint against LabMD alleging that it “failed to provide reasonable and appropriate security for personal information on its computer networks.” FTC did not name an individual complainant and has not discovered anyone harmed by this alleged failure. Despite LabMD’s admitted compliance with HIPPA and HITECH and the massive discovery already undertaken, FTC is now using discovery tactics that would not be tolerated by any Article III court to ruin LabMD’s reputation and business.<sup>4</sup>

### ARGUMENT

The third-party subpoenas wrongfully overwhelm, harass, and embarrass LabMD. While the FTC may obtain “discovery to the extent that it may be reasonably expected to yield information relevant to the allegations in the complaint, to the proposed relief, or to the defenses of any respondent”<sup>5</sup> it is prohibited from abusing this power.<sup>6</sup> But this is precisely what FTC has done, for the third-party subpoenas are filled with irrelevant, overly-broad, and oppressive requests and demands for duplicative information that is more easily obtained from LabMD itself.

FTC is retaliating against LabMD for its CEO’s criticism of the FTC in his recent book, *The Devil Inside the Beltway*. Nothing else explains why the FTC would issue more than thirty-five (35) subpoenas at issue here. Instead of standing on the strength (or lack thereof) of its

---

<sup>3</sup> FTC seeks to depose both witnesses again. *Cf.* FRCP 30(a)(2)(A)(ii)(leave of court required).

<sup>4</sup> LabMD’s counsel suggested the parties agree to ten depositions per side, tracking FRCP 30(a)(2)(A). FTC refused, instead noticing twenty depositions across the country.

<sup>5</sup> 16 C.F.R. § 3.31(c)(1); *see FTC v. Anderson*, 631 F.2d 741, 745 (D.C. Cir. 1979).

<sup>6</sup> 16 C.F.R. § 3.31(d).

Complaint, the FTC seeks to crush LabMD by using its vast resources to harass through abusive discovery tactics.<sup>7</sup>

1. The third-party subpoenas are substantially unnecessary and irrelevant.

Discovery must “reasonably be expected to yield information relevant to the allegations of the complaint, to the proposed relief, or to the defenses of any respondent.”<sup>8</sup> Third-party subpoenas must have a stronger showing of relevance than party discovery,<sup>9</sup> for courts attach greater significance to sweeping nonparty discovery.<sup>10</sup> The subpoenas must seek “generally relevant” information and relevancy is determined by laying the subpoena alongside the pleadings.<sup>11</sup>

Because no one was “injured” by Tiversa taking the PI file (except for LabMD), the Complaint was issued without a complaining witness.<sup>12</sup> Essentially, it alleges that LabMD “failed to provide reasonable and appropriate security for personal information on its computer networks” because Tiversa took the PI file.<sup>13</sup> It says LabMD engaged in practices “that, *taken together*, failed to provide *reasonable and appropriate* security for personal information on its computer networks”; its “information security program” was not “*comprehensive*” and it did not use “*readily available measures*” for e-mail security; it did not “use *readily available* measures to identify *commonly known* or *reasonably foreseeable* security risks” and “could not

---

<sup>7</sup> See FRCP 16, 26(b)(2),30(a)(2),40(c).

<sup>8</sup> 16 C.F.R. § 3.31(c)(1); see *Anderson*, 631 F.2d at 745.

<sup>9</sup> *Echostar Communications Corp. v. News Corp.*, 180 F.R.D. 391, 394 (D. Colo. 1998); *Bio-Vita, Ltd. v. Biopure Corp.*, 138 F.R.D. 13, 17 (D. Mass. 1991)(usual relevance standard does not apply to nonparties).

<sup>10</sup> See, e.g., *Concord Boat Corp. v. Brunswick Corp.*, 169 F.R.D. 44, 48-49 (S.D.N.Y. 1996)(nonparty witness entitled to consideration of expense and inconvenience).

<sup>11</sup> *In the Matter of Rambus Incorporated*, 2002 FTC LEXIS 90, \*4-5 (Nov. 18, 2002)(quoting *In re Kaiser Aluminum & Chemical Corp.*, 1976 FTC LEXIS 68, at \*4 (Nov. 12, 1976)).

<sup>12</sup> The Complaint is attached as Exhibit 2.

<sup>13</sup> *Id.* at ¶¶ 10 (emphasis added).

*adequately* assess” data-security risks; it “did not use *adequate* measures,” “did not *adequately* train employees,” and “did not employ *readily available measures*” relating to data-security; and it “could have corrected its [alleged] security failures at *relatively low* cost using *readily available* security measures.”<sup>14</sup>

The Complaint does not define what is “adequate,” “readily available,” “reasonably foreseeable,” “commonly known,” or “relatively low cost.” It does not specify the regulations LabMD violated or what of LabMD’s alleged failures, “taken together,” violate Section 5. It does not allege that LabMD’s claimed “security failures” caused any so-called “consumers” to suffer economic injury.<sup>15</sup>

The Complaint says that LabMD’s “Day Sheets and a small number of copied checks” were found by the Sacramento Police “in the possession of individuals who pleaded no contest” to identity theft charges.<sup>16</sup> But it does not allege this caused LabMD’s “consumers” injury, speculating only that this “may indicate” such theft.<sup>17</sup>

FTC’s irrelevant third-party discovery falls into three categories:

1. Requests about the Sacramento incident;
2. Requests that are overly broad in time or as to the Complaint’s allegations;
3. Requests regarding contracts.

The Sacramento incident involved a criminal case where Erick Garcia and Josie Maldonado were found with LabMD patient information “Day Sheets.” They pled “no contest” to the unauthorized use of personal identifying information. The Day Sheets were available only

---

<sup>14</sup> *Id.* at ¶¶ 10-11 (emphasis added).

<sup>15</sup> *See id.* ¶11, ¶¶17-20.

<sup>16</sup> *Id.* at ¶21.

<sup>17</sup> *Id.*

in hard copy, not on LabMD's computer network.<sup>18</sup> Discovery of the Sacramento incident is not "strongly relevant" to LabMD's computer network security and all subpoenas with respect thereto, including Erick Garcia, Karalyn Garnett, Josie Maldonado, and the Sacramento Police Department, should be barred.

Furthermore, all subpoenas requesting documents outside of the relevant time period of 2005-2008 are overly broad. FTC cannot show that documents outside this timeframe are relevant, and certainly not strongly relevant, to appropriate computer network security. Therefore, they should be barred.

FTC's request for "all communications between you and LabMD" is not reasonably limited to the Complaint's allegations and should be barred.

FTC seeks discovery of technology and software that LabMD used and currently uses to secure its computer network. However, the parties do not dispute how and when Tiversa took the PI file, as Commissioner Rosch explained; thus, LabMD's technology and software, other than that in place at the time of the events in Complaint paragraphs 17-20, is irrelevant and discovery with respect thereto should be barred.

FTC requests information regarding IT contract services. However, the agreements LabMD had or has with its IT service providers will not shed any new light on the Complaint's allegations. Thus, all such requests should also be barred.

2. The discovery is duplicative.

Third-party discovery may not be "duplicative"<sup>19</sup> and shall be limited where the "burden and expense of the proposed discovery on a party or third party outweighs its likely benefit."<sup>20</sup>

---

<sup>18</sup> See Affidavit of Michael Daugherty, attached as Exhibit 3.

<sup>19</sup> 16 C.F.R. § 3.31(c)(2)(i).

<sup>20</sup> 16 C.F.R. § 3.31(c)(2)(iii).

Here, the documents and depositions sought by the FTC are duplicative, and the burden and expense outweighs the likely benefit, so a protective order is warranted.

The FTC has requested thousands of documents from dozens of parties, many of which have already been provided by LabMD.<sup>21</sup> The requests listed below are wrongly duplicative and need not be reproduced.<sup>22</sup>

1. Documents sufficient to show version(s) and capabilities of any software the Company sold, provided, installed, updated, or maintained on LabMD's network, including, but not limited to operating system software, data backup software, database software, billing software, or antivirus software;
2. Documents sufficient to show how the software sold, provided, installed, updated, or maintained for all software the Company sold, provided, installed, or updated;
3. Documents sufficient to show the settings the Company configured, maintained, updated, or deployed on LabMD's network was configured, including setting provided by the Company at the time the software was sold, provided, installed, updated, or maintained for LabMD;
4. Documents sufficient to show any hardware the Company sold, provided, or installed for LabMD, including, but not limited to servers, workstation computers, firewalls, routers, or switches;
5. Identify by name and job title all Person with authority from LABMD to access Personal Information regarding Consumers, including, but not limited to, Persons who perform tasks related to billing by LABMD for services provided;
6. For each Person identified as having access to Personal Information, state the types of Personal Information that the Person had authority to access;
7. All forensic reports or analysis relating to any security incident.

16 C.F.R. § 3.31(c)(2)(iii) prohibits discovery when the "burden and expense of the proposed discovery on a party or third party outweigh its likely benefit." Because there is no benefit to FTC receiving information it already possesses, almost any burden would be too high,

---

<sup>21</sup> Attached as Exhibit 4.

<sup>22</sup> See *Act, Inc. v. Sylvan Learning Sys., Inc.*, 1999 U.S. Dist. LEXIS 7055 (E.D. Pa. May 14, 1999)(no substantial need for non-party's market information, where that information could be obtained from its own internal research).



especially as a third-party's burden is weighed more heavily.<sup>23</sup> LabMD has already spent hundreds of hours compiling and producing the required documents. The time and resources already expended by LabMD demonstrates the burden that FTC seeks to impose.

FTC cannot justify demanding nonparties produce documents previously produced by LabMD. The allegations of the Complaint surely do not justify this broad inquiry. Therefore, the requested protective order should be granted and the subpoenas barred.

3. The information is more easily obtainable from LabMD.

Under Rule of Practice 3.31(c), discovery "shall be limited" if it is "obtainable from some other source that is more convenient, less burdensome or less expensive."<sup>24</sup> Subpoenas should not be enforced where the information is as easily obtainable from a party to the action as a third party. FTC must demonstrate that the requested information can only be uniquely satisfied by the subpoenaed party to justify third-party production.<sup>25</sup>

FTC has requested:

1. All communications between the third party and LabMD;
2. All contracts between the third party and LabMD;
3. All documents related to compensation received by the third party for services provided to LabMD;
4. Communications between the third party and LabMD regarding any security incident;
5. Identify each inquiry or investigation by a state or federal agency into LabMD's security practices;

---

<sup>23</sup> *Echostar Communic'ns Corp. v. News Corp.*, 180 F.R.D. 391, 394 (D. Colo. 1998)(citations omitted).

<sup>24</sup> 16 C.F.R. § 3.31(c); *see also In re James Carpets, Inc.*, 81 F.T.C. 1062 (1972)(denying ALJ's recommendation that the FTC enforce subpoena).

<sup>25</sup> *See Schering Corp. v. Amgen, Inc.*, 1998 U.S. Dist. LEXIS 13452, at \*8-9 (Aug. 4, 1998).

6. State the names of all Consumers who requested credit monitoring services after receiving a Communication from LabMD related to any Security Incident; and
7. State, as a percentage of the total number of Consumers whose samples LabMD has tested, the proportion of Consumers who:
  - a. are uninsured,
  - b. have commercial health insurance,
  - c. have Medicare, and
  - d. have Medicaid.

FTC has not shown such information cannot be obtained from other sources, including LabMD. Furthermore, requests 1, 2, 3, 6, and 7 have nothing whatever to do with this case. The FTC has no need for this information in a patient-information data-security case, and so this request is made solely to punish LabMD's customers. The government's overreach must not stand.

4. The depositions sought by the FTC have limited benefit in comparison to the cost LabMD would expend to defend them, and are overall oppressive to LabMD.

In addition, FTC seeks to depose more than twenty (20) of LabMD's current and former employees, clients, and IT service providers. Not only is the testimony that FTC seeks duplicative of the information that it already has in its possession for reasons mentioned *supra*, but it is also duplicative of the documents simultaneously requested from these same third-parties. Furthermore, many of the depositions are noticed for varying locations across the country.<sup>26</sup> The expense that LabMD would expend in defending more than twenty depositions cross-country would be astronomical, and outweigh the sparse benefit, if any, that FTC would receive from the testimony. Thus, LabMD respectfully requests that the subpoenas for depositions also be barred.

---

<sup>26</sup> LabMD attempted to limit the number of depositions to 10 depositions each (the limit in federal court absent leave of court). *See* FRCP 30(a)(2)(A). FTC refused.

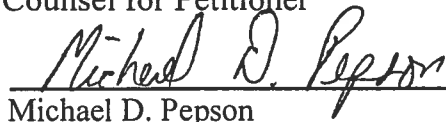
CONCLUSION

Petitioner respectfully requests a protective order to shield LabMD from FTC's oppressive tactics.

Respectfully submitted,



Reed D. Rubinstein  
William A. Sherman, II  
Dinsmore & Shohl, LLP  
801 Pennsylvania Ave., NW Suite 610  
Washington, DC 20004  
Phone: (202) 372-9100  
Facsimile: (202) 372-9141  
Email: reed.rubinstein@dinsmore.com  
Counsel for Petitioner



Michael D. Pepson  
Cause of Action  
1919 Pennsylvania Ave., NW, Suite 650  
Washington, D.C. 20006  
Phone: 202.499.4232  
Fax: 202.330.5842  
Email: michael.pepson@causeofaction.org

*per telephone  
authorization*

Admitted only in Maryland.  
Practice limited to cases in federal court and  
administrative proceedings before federal  
agencies.

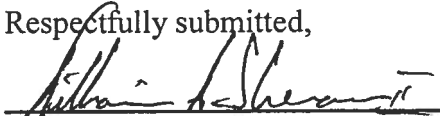
UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION  
OFFICE OF ADMINISTRATIVE LAW JUDGES

\_\_\_\_\_  
In the Matter of )  
 )  
 )  
LabMD, Inc., )  
a corporation. )  
\_\_\_\_\_ )

DOCKET NO. 9357  
  
PUBLIC

STATEMENT PURSUANT TO SCHEDULING ORDER

Pursuant to the Additional Provisions set forth in paragraph 4 of the Scheduling Order, Counsel for the moving party, Respondent, LabMD, Inc. ("LabMD"), hereby certifies that counsel met and conferred with Complaint Counsel in a good-faith effort to resolve by agreement the issues set forth in LabMD's Motion for a Protective Order, but the parties were unable to reach agreement.

Respectfully submitted,  
  
Reed D. Rubinstein  
William A. Sherman, II  
Dinsmore & Shohl, LLP  
801 Pennsylvania Ave., NW Suite 610  
Washington, DC 20004  
Phone: (202) 372-9100  
Facsimile: (202) 372-9141  
Email: reed.rubinstein@dinsmore.com  
Counsel for Respondent

Dated: November 5, 2013

UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION  
OFFICE OF THE ADMINISTRATIVE LAW JUDGES

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

**[PROPOSED] ORDER GRANTING RESPONDENT LABMD, INC.’S MOTION FOR A PROTECTIVE ORDER**

This matter came before the Administrative Law Judge on November 5, 2013, upon a Motion for a Protective Order (“Motion”) filed by Respondent LabMD, Inc. (“LabMD”) pursuant to Commission Rule 3.31(d), 16 C.F.R. §3.31(d), for an Order protecting LabMD from Complaint Counsel’ discovery requests. Having considered LabMD’s Motion and all supporting and opposition papers, and good cause appearing, it is hereby ORDERED that LabMD’s Motion is granted and a protective order is issued barring all third-party discovery requests.

ORDERED:

\_\_\_\_\_  
D. Michael Chappell  
Chief Administrative Law Judge

Date:

## CERTIFICATE OF SERVICE

I hereby certify that on November 5, 2013, I hand-delivered the foregoing document to:

Donald S. Clark, Esq.  
Secretary  
Federal Trade Commission  
600 Pennsylvania Ave., NW, Rm. H-113  
Washington, DC 20580

I also certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

The Honorable D. Michael Chappell  
Chief Administrative Law Judge  
Federal Trade Commission  
600 Pennsylvania Ave., NW, Rm. H-110  
Washington, DC 20580

I further certify that I delivered via electronic mail and first-class mail a copy of the foregoing document to:

Alain Sheer, Esq.  
Laura Riposo VanDruff  
Megan Cox  
Margaret Lassack  
Ryan Mehm  
Division of Privacy and Identity Protection  
Federal Trade Commission  
600 Pennsylvania Ave., N.W.  
Mail Stop NJ-8122  
Washington, D.C. 20580

I certify that the copy hand-delivered to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

Dated: November 5, 2013

By:   
Catherine Chae