UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, DC

Office of the Secretary

June 21, 2012

BY E-MAIL AND COURIER DELIVERY

Stephen F. Fusco, Esq.
LabMD
2030 Powers Ferry Drive
Building 500, Suite 520
Atlanta, GA 30339
sfusco@labmd.org

RE: *Request for Full Commission Review of Denial of Petitions to Limit or Quash the Civil Investigative Demand by LabMD, Inc. and Michael J. Daugherty (FTC File No. 1023099)*

Dear Mr. Fusco:

This letter advises you of the Commission's disposition of LabMD, Inc.'s and Michael J. Daugherty's request dated April 25, 2012, that the full Commission review the denial of their petition to limit or quash civil investigative demands.

The Commission issued the CIDs to LabMD and Mr. Daugherty on December 21, 2011. LabMD and Mr. Daugherty filed petitions to limit or quash the CIDs, which were received by the Commission on January 10, 2012. On April 20, 2012, Commissioner Brill directed the issuance of a letter denying both petitions and directing both petitioners to comply by May 11, 2012. That deadline was extended to June 8, 2012 due to emergency circumstances that you brought to the Commission's attention.[21]

The Commission affirms the ruling denying the petitions to limit or quash the civil investigative demands. The Commission has independently reviewed LabMD and Mr. Daugherty's petitions to limit or quash the CIDs, and their requests for full Commission review. The Commission has also reviewed the letter ruling issued by the Commission at the direction of Commissioner Brill, and hereby affirms that ruling, finding its conclusions to be valid and correct.

[21] On April 30, 2012, you contacted the Commission's Office of the Secretary to request additional time to comply with the CID due to emergency circumstances. By letter dated May 7, 2012, the Commission modified the date to June 8, 2012.

Commissioner Rosch generally agrees with the Commission's decision to enforce the CIDs, but dissents from this ruling to the extent it permits staff to rely on a LabMD document found on a peer-to-peer file sharing network, out of concern about petitioners' allegations that a third party located this document through wrongdoing and for financially-motivated reasons. In this ruling, we make no findings of fact regarding that third party's conduct or the admissibility of this document, nor do we need to do so. In upholding the CIDs, the Commission allows staff to continue to use pertinent information—including information from or concerning any LabMD documents made available to users of peer-to-peer file-sharing networks and accessed by any third party—to conduct its data security investigation. Indeed, in our data security investigations, the Commission often uses information obtained by third parties concerning security vulnerabilities of entities that maintain substantial amounts of personal information. Although we understand petitioners have alleged that the third party in question has a financial incentive to use its patented monitoring tool to find information that has been improperly disclosed on peer-to-peer file sharing networks, that does not overcome the Commission's compelling public interest in seeking to protect consumers' sensitive health data by pursuing this investigation through all lawful means, including the use of this document.

The April 25, 2012 request for full Commission review also requested a hearing on the denial of the petitions. The FTC Rule governing petitions to quash or limit, 16 C.F.R. § 2.7, does not provide for such a hearing, however, and accordingly, this request will be denied.

For the forgoing reasons,

IT IS ORDERED THAT the April 20, 2012 letter ruling is **AFFIRMED**;

IT IS FURTHER ORDERED THAT LabMD's and Mr. Daugherty's request for a hearing is **DENIED**;

IT IS FURTHER ORDERED THAT Commission staff may reschedule the investigational hearings of LabMD and Michael J. Daugherty at such dates and times as they may direct in writing, in accordance with the powers delegated to them by 16 C.F.R. § 2.9(b)(6)(2012); and

IT IS FURTHER ORDERED THAT all other responses to the specifications in the Civil Investigative Demands to LabMD, Inc. and Michael J. Daugherty must be produced on or before June 8, 2012.

By direction of the Commission, Commissioner Rosch dissenting, and Commissioner Ohlhausen not participating.

Donald S. Clark
Secretary

EXHIBIT
19

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FEDERAL TRADE COMMISSION	)	
	)	
Plaintiff,	)	CIVIL ACTION FILE
	)	NO. 1:12-CV-3005-WSD
v.	)	
	)	ATLANTA, GEORGIA
LabMD, INC., et al.	)	
	)	
Defendants.	)	
	)	

TRANSCRIPT OF PROCEEDINGS
BEFORE THE HONORABLE WILLIAM S. DUFFEY, JR.,
UNITED STATES DISTRICT JUDGE

Wednesday, September 19, 2012

APPEARANCES OF COUNSEL:

For the Plaintiff:	FEDERAL TRADE COMMISSION (By: Burke W. Kappler Ryan Thomas Holte Bradley D. Grossman)
For the Defendants:	BALCH & BINGHAM (By: Christopher S. Anulewicz)
	LabMD, INC. (By: Stephen Frank Fusco)

Proceedings recorded by mechanical stenography
and computer-aided transcript produced by
NICHOLAS A. MARRONE, RMR, CRR
1714 U. S. Courthouse
75 Spring Street, S.W.
Atlanta, GA 30303
(404) 215-1486

Wednesday Morning Session

September 19, 2012

10:01 a.m.

-- -- --

P R O C E E D I N G S

-- -- --

(In open court:)

THE COURT: Good morning, everybody. This is a show cause hearing in FTC v. LabMD, Inc., which is Civil Action No. 12-3005.

Would counsel please announce their appearances?

MR. KAPPLER: Good morning, Your Honor. For the FTC, Burke Kappler, to my right is Ryan Holte and Bradley Grossman.

THE COURT: Good morning.

MR. FUSCO: For the respondents, Stephen Fusco with LabMD, and to my left, Chris Anulewicz with Balch & Bingham, and that's Michael Daugherty.

THE COURT: Good morning.

I haven't had a lot of time to look at the briefs, but I have looked at the briefs, and I just want to frame the issue as it strikes me.

It looks to me -- and I have done this enough to know the deferential responsibility I have to administrative agencies conducting investigations. It's

about the same in this kind of action by the FTC as it would be in others.

So my understanding and my belief is that regulatory agencies have broad authority to do certain things, and when they are within that broad authority, they can do a lot of things, one of which is to conduct these sorts of investigations. And the general rule in my mind is that when that happens, if you are asked to produce information, you have to.

I don't think that's the issue in this case. I think the issue in this case, now having read Section 45 and having read the 2008 resolution, is a question of whether or not this is within the authority of the FTC.

I haven't done any independent research as I would normally do if I had more time for that, so I'm just looking at broad 25,000-foot issues.

It's not entirely clear to me, but it does look like this fundamental is the FTC acting within the scope of its authority under Section 45 was the subject of the initial objections through the Commissioner/Commission process.

In fact, I think even in the submission by the FTC that started this action, they said in their petitions LabMD, Mr. Daugherty, raised a number of claims challenging the FTC's authority to investigate their data security

practices. And so the FTC has made that representation to me.

So we go through the regular administrative practices route or administrative challenge route and you get a decision out of the Commission. So the first question I have is if in fact the general question of whether or not the information being requested of LabMD was within the authority of the Commission, at the Commission level, after that decision, does a party have a right to go somewhere at that point to challenge the Commission's decision.

Because it seems to me that what the Commission is saying is we passed this 2008 resolution. You are saying that we couldn't do that. We wouldn't have passed the resolution unless we thought we could do that. So, therefore, that's why -- the reason why we think that by acting pursuant to the resolution, that we were acting within our authority.

I'm just -- it just seems to me at that point, because of the nature of that process, that a party ought to have a right to say, well, I don't agree with that, and I would like somebody who is fair and objective -- i.e., a district court or whatever federal court has authority when -- and I don't know who does.

So the first question I have is did LabMD at that point have a further review or recourse to challenge their --

to assert their claim that what was being asked was not within the agency's authority.

That's important to me, because then it raises the question of, them not doing that, was that challenge not waived.

Now -- but then I said to myself, well, then there are all these cases where they challenged investigative CIDs, and all those cases say, well, the fundamental question, the first question that a court has to evaluate is that you have to enforce it, but it has to be within the authority of the agency.

So I thought, well, maybe this is the right process, maybe this is where those issues are supposed to be raised. But I will say I don't know the answer to that.

So where I want to focus this morning and before I even get to -- I think before I can get to the enforcement issues is that I have to make sure I understand and correctly decide the within the jurisdiction of the agency issue.

And I don't know, and I apologize for not sending you something beforehand to tell you that we could have put this off and we could have taken another week and I could have focused on that, we could have come back and I could have been more informed and better prepared, but I didn't do that.

So thank you for coming. I assume you traveled from Washington. I got you out of town, and it's always a good town to get out of.

So maybe we can have that discussion now, which is in your view -- I know that you are going to disagree with what LabMD is saying. What I need to know is I need to just have that disagreement presented to me with the right authority so that I can study it.

And I thought the best discussion to have would be how can I have you help me do that. Does that make sense?

MR. KAPPLER: It does, Your Honor.

THE COURT: So how can I have you help me do that?

MR. KAPPLER: Well, Your Honor, would you like me to address the questions that you have raised and perhaps begin the discussion?

THE COURT: That would be great. That would be fine.

MR. KAPPLER: Your Honor, would you prefer if I address you from here or should I come to the podium?

THE COURT: You know, it's probably -- you have got your stuff all laid out there, and these are great microphones. So I don't -- you don't speak with any more authority by walking three feet and standing at the podium.

MR. KAPPLER: Thank you, Your Honor. I appreciate

that.

Well, Your Honor, thank you. May it please the Court, we actually appreciate the Court's speedy time frame for this proceeding, and I understand you would like to have more time to review --

THE COURT: You mean I could have taken longer?

MR. KAPPLER: Well, we do. These are meant to be summary proceedings, and we really appreciate the Court's attention to that fact.

Responding to the question -- you posed a couple of questions. One deals with the FTC's authority over this area, but more importantly you asked the question does the party have the right to raise these claims of authority after the FTC has completed its review of the petitions to limit or quash.

And the answer is not really, Your Honor. Because as the case law explains, this proceeding before you today is really a question of whether the CIDs should be enforced.

The question of whether the FTC has the regulatory coverage or the jurisdiction to actually engage in this or actually to conduct a law enforcement action comes later if we were to in fact then bring a complaint or bring an action or bring an enforcement action against LabMD, which is a decision that has not been made yet.

At that point, LabMD would have recourse to argue

it went outside of the FTC's jurisdiction.

THE COURT: I understand. I'm not sure I totally agree with your -- as a practical matter, as a legal matter, I agree with that general statement, although I understand why you are making the statement.

Because even if you go to our circuit, in '91 when they are looking -- and that was an EEOC case in *Kloster Cruise* -- and it's probably -- maybe the language would be a little different if I had run across an FTC case, but it seems that even when you are in the enforcement process, that fundamentally I have to be satisfied that there is some jurisdictional hook.

And I think there was a case out of the D.C. Circuit involving cigarette labeling. *Carter* I think is the case.

MR. KAPPLER: Yes, sir, *Carter*.

THE COURT: In *Carter,* just looking at the discussion, it appeared that that was an enforcement action, but one of the things that the court did there is, well, let me start to see whether or not there is a grant of authority to the FTC, and that was a lot clearer because the Cigarette Labeling Act specifically granted to the Commission certain -- and they said there it's clear to us the FTC is doing what they are supposed to be doing.

So I think as a general legal principle that I have

to at least do some testing of whether or not what's being investigated is within the authority of the agency.

And just this morning in talking in my chambers, I said because theoretically if -- you know, I don't think the FTC is saying this, but that's because you are a trustworthy lawyer, but there might be other lawyers who are maybe a little more loose with the granted authority that's given.

If the argument is if it's within interstate commerce and it's a practice, then we get to investigate it, well, I could make an argument that a trucking company and the way that they drive trucks over the interstate highway system is -- the driving of trucks is a practice. Whether they do it safely is within interstate commerce, so I can go ahead and issue a CID because I'm investigating drivers' practices on interstate highways.

And then you could do all that, come back and say, well, you know, we have decided we are not going to bring it. Or you say, you know, we have decided the ABC Trucking Company, the practice in which they are engaged in in which they buy trucks, that we have looked at who they hire to drive and the kind of trucks, and we don't think that's the right fit, we are going to bring an action.

And to think that at that point when a complaint is brought, for somebody to say, wait a minute, that goes way

too far, that's not within their jurisdiction, but they have already spent a quarter of a million dollars complying, the court might say, you know, that's right, I don't think that that's what the Section 45 grants to the FTC.

MR. KAPPLER: Well, to be specific, Your Honor, I mean, the hypothetical you have offered, I believe that there is actually a cut-out of FTC jurisdiction for common carriers like --

THE COURT: Well, if you give me more time, I will come up with another example.

MR. KAPPLER: No. But to be clear, Your Honor, I mean, the FTC's jurisdiction is to investigate unfair or deceptive acts or practices in or affecting commerce. And when Congress wrote that language, they did so with the expectation that the Commission would apply it flexibly.

In fact, if you look at some of the cases we've cited --

THE COURT: I agree with all that.

MR. KAPPLER: Okay.

THE COURT: The question is whether or not this is -- but it didn't say it could do it indiscriminately and expansively by just saying I found something in interstate commerce and I found a practice.

MR. KAPPLER: No, Your Honor, it didn't say that. But the point is that the question I think at issue here

is -- the subject of this investigation involves, for example, data security. Does the Commission have the ability to investigate data security under its Section 5 grant of authority, and the answer is yes. And there really isn't anything that anyone can point to where the answer would be no, as a matter of fact.

But getting back to where we started, Your Honor, you looked at *Kloster Cruise,* for instance, from 1991. I mean, I think that case is a great example of the exact -- of the level of analysis that needs to be done here.

Because in that case, what the court said was as long as there is just a plausible argument for jurisdiction, the court should deal with the investigatory issue and let the case proceed to the merits.

And there is a real reason why we do this.

THE COURT: You might be totally right about that. What I'm saying is I don't have enough research and briefing on that issue to move beyond that today, because I think it has been fairly superficially briefed, because I didn't ask you to do it in more detail.

So I guess what I'm saying is I will tell you right now I'm not prepared to enforce the CIDs today until I answer that fundamental question and --

MR. KAPPLER: Well, Your Honor, it might be worth, if I might, sort of discussing a little bit of the law

here.

I mean, it was not briefed extensively, but it was briefed in the briefs in a way. It was raised by LabMD in their opposition, and we addressed it in our brief.

And, you know, really what it comes down to is, I mean, LabMD is taking the position -- has taken the position that at one point twelve years ago in the course of a single report in one sentence, that the FTC disclaimed or disavowed its authority to look at data security under Section 5.

And, first of all, if you read that report -- in fact, if you just read the paragraph in that report where that sentence appears --

THE COURT: See, I'm not -- you are not hearing me.

MR. KAPPLER: Okay.

THE COURT: That really is not one of the important points that they make, because somebody could have said that and been somebody without authority to have said that, and I don't care.

I'm looking at the law. There is a statute. The statute grants certain authorities. And my personal opinion is that that doesn't mean it's unlimited authority, and that the courts have said that there are some constraints on that.

And I don't -- I have not done personally enough research, and your research has not adequately fleshed this out for me, as to what the scope of that authority is and whether in this particular case there is a sufficient hook to the authority and what the defendant has been told about now the exercise of that authority for me to make sure that if I allow these to be enforced, that -- and this is a personal problem I have is that I really have to be comfortable in making legal decisions and going through the process. Maybe I'm too pedantic about that, but that's my nature, and you got me.

And all I want is more from you discussing the more fundamental issue, including the standard as it applies in this particular case as the FTC is asserting its jurisdiction, to conduct this investigation under Section 45 in this 2008 resolution.

MR. KAPPLER: Well, Your Honor, I want to make sure I understand exactly what you are asking from me. Because I mean, what I can do is I can point you to, for instance, the thirty or forty cases we have already brought applying Section 5 or Section 45 in the data security or consumer privacy context.

I can point you to the fact that we have testified to Congress on numerous occasions and told Congress that we view Section 5 as authorizing us to investigate and bring

enforcement actions under -- involving data security and consumer privacy.

We have spoken on panels. We have conducted workshops. We have published guidance for businesses just like LabMD about our view that data security practices can be enforceable under Section 5 if they become unfair or deceptive in some form or fashion. I mean, really --

THE COURT: Do you have any Eleventh Circuit authority or any authority out of my circuit --

MR. KAPPLER: No, Your Honor.

THE COURT: -- within those 45 cases?

MR. KAPPLER: No, I actually can't point to a case -- out of those 45 cases out of the Eleventh Circuit?

THE COURT: I don't think so.

MR. KAPPLER: No. The issue is, Your Honor, most of them have been settlement, they have not been litigated decisions.

On the other hand, though, there is actually no authority from any court saying that Section 5 does not include data security.

THE COURT: And there is no authority that says Section 5 does include it.

MR. KAPPLER: Yes.

THE COURT: So I'm writing on a blank slate, which is my issue.

MR. KAPPLER: Well, but, Your Honor, I think you can take some comfort from the perspective that, again, you are acting consistent with what Congress intended in the first place, which is flexible, broad authority.

THE COURT: Let me just explain something. I'm not here to be comforted. I'm here to do my duty as a judicial officer to interpret the law.

I'm trying as politely as I can tell you that, one, I am not enforcing these CIDs today. I'm asking for your cooperation. And if you need more direction, I'm happy to send you an e-mail telling you specifically the issue that I need addressed.

And that's what I would have done if I had been more thoughtful about this and realized that that's a fundamental issue that I have.

But I'm going to address that fundamental issue. I'm going to do it probably in a written order so that if anybody wants to complain about it to another court, that they will know at least what my reasoning was.

And I think that -- I think based upon my initial review of this that that is -- one of the issues is nobody really has litigated your authority in this area to do this, although you apparently have done a lot of it. That that doesn't mean a party doesn't have a right to raise a legal issue before me and have me decide it.

MR. KAPPLER: Oh, Your Honor, we don't disagree with that. But I think -- I understand your duty as a judicial officer, but I think the Eleventh Circuit has spoken clearly about what a court like this should do in a proceeding like this and the test that it needs to apply.

And that test comes out of *Kloster Cuise,* it comes out of *Genuine Parts v. FTC* from 1971, Fifth Circuit for that case actually.

THE COURT: I'm real good about following what my circuit tells me to do.

MR. KAPPLER: Right.

THE COURT: But I'm also real good about doing it in a way in which I am comfortable that I'm following it with integrity and properly.

MR. KAPPLER: Understood, Your Honor.

Well, Your Honor, let me --

THE COURT: This is only a process -- this is supposed to be a discussion about that process.

MR. KAPPLER: Well, Your Honor, let me put it this way. You are asking me and what I understand you to be saying is can you point me to a case that says my court, preferably in the Eleventh Circuit or even in Georgia, that says the FTC has the authority to investigate data security under Section 5. And the answer is I cannot point you to that case. It doesn't exist, not to my knowledge.

I also, though, can't point you to a case that says the FTC does not have authority under Section 5 to investigate data security in consumer practices.

THE COURT: So what we are going to have to do is we are going to have to go and look at authorities in other contexts to get the contours of the analysis that a district court is supposed to undertake to determine whether or not a grant of authority in an area is within Section 45 and that the passage of a resolution was properly exercised, and now an investigation is being appropriately conducted pursuant to that resolution under Section 45, because that's the original grant of authority.

MR. KAPPLER: Right.

THE COURT: And I know none of you have addressed that, but we need to. That's all I'm saying.

MR. KAPPLER: Well, again, Your Honor, I keep coming back to the fact that, you are right, I mean, the scales balance out, the case law balances out on the plain question at issue.

But on one side, though, there is ample case law discussing the broad grants of authority that have already been given to the FTC by Congress so that in questions like this, in questions where courts are asking what is the FTC's authority, there is a tendency and a deference to the Commission in the finding.

THE COURT: I know. You know, but if that's the case, then why did my friends at the D.C. Circuit write a published opinion in *Carter* going through the analysis? If it is so plain on its face that you can stand up here and I am supposed to say I confess that you are right, there is at least three other judges -- four other judges that said that was entitled to some deliberation.

MR. KAPPLER: Well, Your Honor, I would also point you to the D.C. Circuit's case in *Texaco,* which was an *en banc* decision by all of them, which granted the FTC broad authority, said that it was not appropriate in stages like this to get into these jurisdictional questions because that would hamper the agency's effectiveness in conducting investigations.

So the balance of that with *Carter* is *Texaco*.

Carter, by the way, also did affirm and enforce the subpoenas at issue in that case.

THE COURT: Because they found a specific grant to the Commission pursuant to a legislative act of Congress that entitled the Commission to conduct the investigation that they were conducting.

MR. KAPPLER: And that is Section 5, Your Honor. In this case, that is Section 5. It is a grant to us to investigate unfair and deceptive acts or practices in or affecting commerce.

The resolution in this case, the one passed in 2008, identifies the area that we are looking at. In fact, it's a procedural safeguard for parties just like LabMD and Mr. Daugherty to say we are using our authority, we are telling you exactly what we want to look at, we want to look at your practices related to privacy and data security.

THE COURT: I think you are just arguing to hear yourself argue right now.

I think what I have tried to tell you is there is a process I want to discuss, and I'm happy to do that. I'm happy to fast track it.

And I know this. And you were nice to say that this was prompt. You would not have had a hearing in this as quickly as you had in this Court in almost any court in the country, so you know that I'm paying attention to this and you know that I have a commitment to this.

What I'm asking for you is if you want that commitment to be maintained, then you need to cooperate in the process.

MR. KAPPLER: Your Honor, I want to fully cooperate in the process.

THE COURT: And you need to look at your colleague who is nodding his head, I think trying to give you a signal that we ought to talk about the process and move on.

MR. KAPPLER: Well, Your Honor, it sounds to me as

though you are suggesting we engage in some sort of further briefing on this issue?

THE COURT: Yes.

MR. KAPPLER: Well, Your Honor, I think we would submit we are happy to do that. If Your Honor needs more information or needs more authority, we are happy to produce that.

I think what we are saying is, as we understand the cases as they apply, that's not necessary, but if Your Honor wants to do that, we are happy to do that.

THE COURT: You know, the day that you become appointed an Article III judge, then you can decide what is or is not necessary. But you are an advocate now.

MR. KAPPLER: Yes, Your Honor.

THE COURT: I'm telling you that I need more information. And we can go from me trying to be collegial about this, or I can just order you to do it. What's your preference?

MR. KAPPLER: Your Honor, I really appreciate the Court's willingness to engage in this dialogue. I would like to be collegial about it. If you would like more briefing, I am happy to do that.

And I would ask the Court then how would you propose for us to do it?

THE COURT: I'm going to send you an e-mail, since

you have this I guess insatiable need to have specificity, because the only -- because you don't think I need this, but I'm telling you I do. So I will send you an e-mail today telling you the specific issues to address.

MR. KAPPLER: And will Your Honor lay out a briefing schedule?

THE COURT: Yes, we will.

MR. KAPPLER: Okay. Does Your Honor anticipate counter-replies and so forth?

THE COURT: I do.

MR. KAPPLER: We are happy to provide that, Your Honor.

THE COURT: Thank you. That's going to be put into place, today.

MR. FUSCO: Thank you, Your Honor.

THE COURT: I don't know why it was so hard to decide upon that.

But you know that the weight of authority is in favor of an investigative agency conducting this sort of process. You have already largely participated in the process.

And I'm telling you that this better be an important issue to you and one in which you probably will appeal for me to go through this process. Because if what we are doing is somehow delaying this because ultimately that

you think it's in your client's best interest to get whatever additional information to let the process move forward, and I find that out later, I will be disappointed.

MR. FUSCO: Yes, Your Honor.

THE COURT: I have a long memory.

MR. FUSCO: LabMD, the Section 5 authority under this issue is extremely important to them, and we are well aware of the novelty of the question being presented.

THE COURT: Well, that will be the process, and you will get instructions and a schedule from me today.

MR. FUSCO: Thank you, Your Honor.

MR. KAPPLER: Thank you, Your Honor.

THE COURT: Thank you for coming.

(Proceedings adjourn at 10:24 a.m.)

C E R T I F I C A T E

UNITED STATES OF AMERICA :
:
NORTHERN DISTRICT OF GEORGIA :

I, Nicholas A. Marrone, RMR, CRR, Official Court Reporter of the United States District Court for the Northern District of Georgia, do hereby certify that the foregoing 23 pages constitute a true transcript of proceedings had before the said Court, held in the city of Atlanta, Georgia, in the matter therein stated.

In testimony whereof, I hereunto set my hand on this, the 19th day of September, 2012.

/s/ Nicholas A. Marrone

NICHOLAS A. MARRONE, RMR, CRR
Registered Merit Reporter
Certified Realtime Reporter
Official Court Reporter
Northern District of Georgia

EXHIBIT

2

PUBLIC

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	)	**DOCKET NO. 9357**
LabMD, Inc.,	)	**PUBLIC**
a corporation.	)	**ORAL ARGUMENT REQUESTED**

RESPONDENT LabMD, INC.'S MOTION TO DISMISS COMPLAINT WITH PREJUDICE AND TO STAY ADMINISTRATIVE PROCEEDINGS

Reed D. Rubinstein, Partner
D.C. Bar No. 440153
Dinsmore & Shohl, LLP
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9120
Fax: 202.372.9141
Email: reed.rubinstein@dinsmore.com

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

Counsel for Respondent LabMD, Inc.

TABLE OF CONTENTS

RESPONDENT LabMD, INC'S MOTION TO DISMISS COMPLAINT WITH PREJUDICE AND TO STAY ADMINISTRATIVE PROCEEDINGS

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

Please take notice that, pursuant to Commission Rule 3.22(a), 16 C.F.R. § 3.22(a), Respondent LabMD, Inc. (LabMD), hereby moves to dismiss the Federal Trade Commission's (the "Commission" or "FTC") Administrative Complaint (the "Complaint") in its entirety with prejudice and to stay all proceedings before the Administrative Law Judge (ALJ) pursuant to Commission Rule 3.22(b), 16 C.F.R. § 3.22(b), while this Motion is under review.

INTRODUCTION

The only federal court to address the legitimacy of the FTC's claimed authority to regulate data-security practices as "unfair" acts or practices under Section 5 of the Federal Trade Commission Act (FTCA), 15 U.S.C. § 45, said "there is significant merit" to the argument that Section 5 does not provide general jurisdiction over data-security practices and consumer-privacy issues.[1] *FTC v. LabMD*, No. 1:12-cv-3005-WSD, Dkt. No. 23, at 6-7 (N.D. Ga. Nov. 26, 2012). When asked to cite a case that "says the FTC has the authority to investigate data security under Section 5," a Commission attorney admitted that "I cannot point you to that case. It doesn't exist…." Hearing Transcript, *FTC v. LabMD*, No. 1:12-cv-3005-WSD, at 16:20-25 (N.D. Ga. Sept. 19, 2012).

[1] The court, noting its "sharply limited" role, explained that the "subpoena enforcement proceeding is not the proper forum" to decide the scope of statutory jurisdiction. *FTC v. LabMD*, No. 1:12-cv-3005-WSD, Dkt. No. 23, at 6-7. It only found that the FTC had made a "plausible" argument that it had jurisdiction to *investigate* whether LabMD had engaged in unfair or deceptive practices. *Id.* at 1-2, 6-7, 12-13 & n.3. Notably, the FTC's Complaint does not allege that LabMD engaged in any deceptive practices whatsoever. *See* Compl. ¶¶22-23.

The FTC has not only repeatedly told Congress that the Commission does not have Section 5 jurisdiction over data-security practices but also repeatedly asked for the broad authority to regulate such practices. Congress, in turn, has repeatedly refused, delegating the FTC only very narrow and limited authority over data-security practices in circumstances that do not obtain here.[2] In fact, Congress has given the Department of Health and Human Services (HHS), and not the FTC, the sole and specific authority to regulate the patient-information data-security practices at issue in this case.

Even the President has rejected the FTC's power-grab approach to data-security regulation.[3] See Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

---

[2] Congress would not have made these specific delegations if it believed that the FTC had general Section 5 authority to regulate patient-information and other data-security practices. Rather, these delegations demonstrate that Congress ratified the Commission's historic understanding of the limits on its Section 5 jurisdiction and confirm that the FTC's Section 5 "unfairness" authority does not extend to the patient-information data-security practices at issue here. *See infra* Section I.B.

[3] The President apparently recognizes that the FTC's "sue now, offer guidance later" approach is bad policy and unconstitutional to boot. His Order requires the Department of Commerce, through the National Institute of Standards and Technology (NIST), to lead the creation of a baseline set of standards for a "Cybersecurity Framework" establishing a "set of standards, methodologies, procedures, and processes" and including implementation "guidance." *See* Exec. Order No. 13,636 § 7(b). The Framework must "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach" with specific "information security measures and controls" operators can implement to "identify, assess, and manage cyber risk." *Id.* NIST must "engage in an open public review and comment process." *Id.* § 7(d).

The FTC's attack on LabMD and other companies is contrary to each of the steps in the President's Executive Order for effective and lawful data-security regulation. The FTC has not (1) issued any standards, methodologies, procedures, or processes for Section 5 compliance; (2) established guidance for measuring implementation and performance of compliant data-security protections; (3) identified specific information security measures and controls that a business might adopt; or (4) engaged in an open public review and comment process. There is simply no reason why the FTC should not be required to follow the President's process of requiring rules, regulations, and standards *before* the government brings abusive enforcement actions and makes shifting and uncertain compliance demands.

The Complaint is a classic example of regulatory overreach and, accordingly, it should be dismissed in its entirety with prejudice for the following reasons.

First, Congress has not given the FTC the power to use its Section 5 "unfairness" authority to do what it has done to LabMD here, and so this action is illegal and illegitimate. *La. Pub. Serv. Com. v. FCC*, 476 U.S. 355, 374 (1986).

Second, even if Section 5 authorized the FTC to broadly regulate data-security practices as "unfair" acts or practices, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), as interpreted and enforced by HHS, control. More recent and more specific than the FTCA, HIPAA and HITECH manifest Congress's unambiguous intent to give HHS regulatory authority over patient-information data-security and to displace whatever Section 5 authority the FTC might have to regulate LabMD's data-security practices as "unfair" acts or practices.

Third, the FTC's failure to promulgate *any* data-security regulations, standards, or guidance that would allow LabMD to ascertain with reasonable certainty what data-security practices the Commission believes Section 5 to forbid or require, and its *ex post facto* enforcement practices, deny LabMD and others similarly situated of fair notice and violate the Constitution and the Administrative Procedure Act (APA).

Fourth, the acts or practices alleged in the Complaint are not "commerce" within the scope of the FTCA.

Fifth, the Complaint couches legal conclusions as factual statements and therefore fails to state a facially plausible claim for relief.

STATEMENT OF FACTS

LabMD is a small medical company providing its physician-customers with cancer diagnoses. These physicians send LabMD their patients' blood, urine, and tissue for sampling, together with relevant patient identification and insurance information. LabMD does the testing and then sends back a diagnosis to the requesting doctor.

LabMD's patient-information data-security practices are, and were at all times relevant, regulated under HIPAA and HITECH. Congress tasked HHS to implement and enforce these statutes, and it has promulgated regulations to do so.[4] LabMD has never been accused of violating HIPAA or HITECH by the FTC, HHS, or anyone else. *See* Initial Pretrial Conference Transcript, *In the Matter of LabMD, Inc.*, Dkt. No. 9357, at 22:10-13 (Sept. 25, 2013)(hereinafter "Trans.").

The genesis of this action appears to have been in early 2008, when, without LabMD's knowledge or consent, Tiversa, Inc. (Tiversa), a government contractor that created and exploited data breaches to generate business, took possession of a single LabMD physician patient-information spreadsheet file (the "PI file"). Complaint, *Tiversa et al. v. LabMD et al.*, Dkt. 1, No. 2:13-cv-01296-NBF, at 4 ¶¶18-19 (W.D. Pa. Sept. 5, 2013)(hereinafter "Tiversa Compl."). Tiversa has boasted to Congress about its practice of taking computer files from unsuspecting third persons without their knowledge or permission using a "unique technology" unavailable to the general public. *See Hearing Before the H. Subcomm. on Commerce, Trade, & Consumer Protection*, 111th Cong. 3-4 (2009)(statement of Robert Boback, CEO, Tiversa).

[4] *See, e.g.*, 42 U.S.C. § 1320d-2(d)(1)("Security standards for health information" established and enforced by HHS); 65 Fed. Reg. 82,462, 82,463 (Dec. 28, 2000)(HHS's HIPAA Privacy Rule); 68 Fed. Reg. 8,334, 8,334 (Feb. 20, 2003)(HHS's HIPAA Security Rule); 78 Fed. Reg. 5,566, 5,639 (Jan. 25, 2013)(HHS's HITECH Breach Notification Rule).

Tiversa said in a May 28, 2009, press release (since pulled from the Internet) that in "a typical day" it might see sensitive information "of tens of thousands" being unknowingly "disclosed" by a hospital or medical billing company, a third-party payroll provider, or a Fortune 500 company. *See* Press Release, "Tiversa Identifies Over 13 Million Breached Internet Files in the Past Twelve Months" (May 29, 2009). It also said that, working with Dartmouth College researchers under a government contract, it searched file-sharing networks for key terms associated with the top ten publicly traded healthcare firms in the country, and "discovered" what it called "a treasure trove of sensitive documents," such as a spreadsheet from an AIDS clinic with Social Security numbers, addresses, and birth-dates; hospital databases with Social Security numbers, contact details, insurance records, and diagnosis information on 20,000 patients; the PI file; and "350+ megabytes of data comprising sensitive reports relating to patients of a group of anesthesiologists."

After taking LabMD's property, Tiversa telephoned LabMD offering "remediation services" and a cost estimate. Tiversa Compl. ¶¶19-21. That same day, Tiversa sent LabMD three follow-up sales-pitch emails. *See LabMD, Inc. v. Tiversa, Inc.*, 509 Fed. Appx. 842, 843 (11th Cir. 2013). Over the next two months, Tiversa sent six more sales-pitch emails to LabMD. *See id.* Communications between LabMD and Tiversa stopped only when "LabMD did not retain Tiversa's services." Tiversa Compl. ¶22.

Tiversa then gave the Commission the purloined PI file. Tiversa Compl. ¶¶25-26. Apparently, the PI file was the only file of those mentioned in Tiversa's Press Release given to the Commission. And, with this file in hand, the FTC began investigating LabMD. After years of intrusive and costly discovery, including multiple civil investigate demands (CIDs),

depositions, and document productions, on August 28, 2013, the Commission voted unanimously to issue the Complaint.

The Complaint alleges that LabMD violated Section 5's prohibition of "unfair" acts or practices by allegedly engaging in data-security practices that, "taken together," fail to meet the Commission's unspecified standards. *See* Compl. ¶10. The Complaint does not allege that LabMD engaged in "deceptive" acts or practices. *Id*. ¶¶22-23. Nor does it allege that any "consumers" have suffered any harm due to the Tiversa take.[5] *Id*. ¶¶17-19. Instead, it alleges in vague, conclusory terms that LabMD engaged in unspecified "unfair acts or practices."

Tellingly, the Complaint does not cite any regulations, guidance, or other standards for what patient-information data-security practices the Commission believes to be "adequate" or "readily available" or "reasonably foreseeable" or "commonly known" or "relatively low cost." *Id*. ¶¶10-11. It does not specify what regulations, guidance, or standards LabMD fell short of or what combination of LabMD's alleged failures to meet these unspecified requirements, "taken together," violate Section 5. *Id*. ¶10. It does not allege that LabMD's claimed "security failures" caused "consumers" to suffer any economic or other injury. *See id.* ¶¶10-11, 17-21.

The Complaint alleges 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 state charges of identity theft." *Id*. ¶21. But it does not allege that those "individuals" in fact used LabMD's Day Sheets and copied checks to engage in identity theft or caused any of LabMD's "consumers" to suffer any injury. *See id.* Instead, the Complaint alleges that "[a] number of the SSNs in the Day Sheets are being, or have been, used by people

[5] As LabMD explained in its Answer, what the Complaint calls LabMD's "consumers" are in reality LabMD's referring physicians' patients. It is these physicians, and not their patients, who are LabMD's customers and the consumers of its diagnostic services.

with different names"—which, even if true, may be mere correlation (the Complaint does not allege any causation)—and speculates that this "*may indicate* that the SSNs have been used by identity thieves." *Id.* (emphasis added).

Asked about other sources of data-security standards, the FTC said the "Commission has entered into almost 57 negotiations and consent agreements that set out a series of vulnerabilities that firms should be aware of, as well as the method by which the Commission assesses reasonableness." Trans. 9:18-22. The FTC pointed to "public statements made by the Commission" and so-called "educational materials that have been provided" as standards. Trans. 9:23-25. In addition, the FTC argued that "the IT industry…has issued a tremendous number of guidance pieces and other pieces that basically set out the same methodology that the Commission is following in deciding reasonableness," except that the "Commission's process" involves "calculation of the potential consumer harm from unauthorized disclosure of information." Trans. 10:1-7. The FTC also referenced "guiding principles" and stated that "[t]here are lots of sources for the principles, such as materials published by the National Institute of Standards and Technology [NIST], continuing education for IT professionals, practical IT experience, and lessons learned from publicized breaches." Trans. 11:21-12:2.

But critically, the FTC did not claim that any of the above has the force of law or creates any binding duties and obligations.

The FTC also accused LabMD of violating Section 5 "by failing to provide reasonable security for sensitive information," opining "that reasonableness is a common sense balancing of cost and benefit and that common sense is available from many, many sources, including organizations—government organizations, such as the National Institute of Standards, private entities, such as the SANS Institute, and many others as well." Trans. 21:19-22:2. But again, the

FTC did not claim that LabMD violated any data-security standards that have the force of law, such as the patient-information data-security regulations implementing HIPAA.

In fact, the FTC has not accused LabMD of violating any data-security statutes, rules, or regulations. At the initial pretrial conference, the ALJ asked: "Are there any rules or regulations that you're going to allege were violated here that are not within the four corners of the complaint?" Trans. 22:10-12. The FTC responded "No." Trans. 22:13. The FTC also admitted that "[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward." Trans. 20:15-17. The FTC has never promulgated patient-information data-security regulations, guidance, or standards under Section 5 and, apparently, it has no plans to do so: "[T]here is no rulemaking, and no rules have been issued, other than the rule issued with regard to the Gramm-Leach-Bliley Act…for financial institutions." Trans. 10:11-15.

STANDARD OF REVIEW

A Respondent may raise jurisdictional and other legal defenses in a motion to dismiss, which is treated like a Fed. R. Civ. P. 12(b)(6) motion for failure to state a claim upon which relief can be granted. *In re Union Oil Co.*, 138 F.T.C. 1, 16 (F.T.C. 2004). The FTC bears the burden of establishing jurisdiction. *See* Commission Rule 3.43(a), 16 C.F.R. § 3.43(a); *In re POM Wonderful LLC*, 2012 FTC LEXIS 106, 463-65 (F.T.C. May 17, 2012)(Initial Decision). It may not do this by pleading legal conclusions, as it has done here. "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Instead, there must be facts showing grounds for a plausible claim for relief, not merely labels and conclusions and a formulaic recitation of the elements. *Id. at 679; Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

ARGUMENT

I. THE COMMISSION LACKS SECTION 5 "UNFAIRNESS" AUTHORITY TO REGULATE PATIENT-INFORMATION DATA-SECURITY PRACTICES.

Section 5 prohibits unfair acts or practices in or affecting commerce. 15 U.S.C. § 45(a)(1). The Commission does not have carte blanche to regulate anything and everything it unilaterally deems "unfair." *See, e.g., Scientific Mfg. Co. v. FTC*, 124 F.2d 640, 644 (3d Cir. 1941)(holding that Section 5 does not authorize the Commission to regulate publications "concerning an article of trade by a person not engaged or financially interested…in that trade," because otherwise it "would become the absolute arbiter of the truth of all printed matter"). In fact, in 1994 Congress enacted limiting language to control the FTC's misuse of its Section 5 unfairness authority. *See* 15 U.S.C. § 45(n); Howard Beales III, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, 22 J. PUB. POL'Y & MKTG. 192 (2003)(former Director of FTC's Bureau of Consumer Protection describing how Congress "reigned in" Commission "abuse" of its Section 5 unfairness authority), *available at* http://www.ftc.gov/speeches/beales/unfair0603.shtm (accessed Nov. 7, 2013).

The FTC must show that it has congressionally delegated authority to regulate LabMD's patient-information data-security practices. *City of Arlington v. FCC*, 133 S. Ct. 1863, 1869 (2013)(agencies' power to act and how they are to act is authoritatively prescribed by Congress, so when they act beyond their jurisdiction, what they do is ultra vires); *see, e.g., ABA v. FTC*, 430 F.3d 457, 468-71 (D.C. Cir. 2005)(holding that the FTC's interpretation of the Gramm-Leach-Bliley Act to authorize it to regulate attorneys engaged in the practice of law exceeded the Commission's statutory authority and was therefore invalid). And, the law requires the FTC to exercise its Section 5 unfairness authority consistent with the congressionally enacted administrative structure. *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 125, 133

(2000). Finally, the controlling authorities hold the scope of Section 5 authority must be viewed in the light of other relevant statutes, "particularly where Congress has spoken subsequently and more specifically to the topic at hand."[6] *Id.* at 133; *see also FTC v. Nat'l Cas. Co.*, 357 U.S. 560, 562-63 (1958), *superseded by statute* (examination of subsequent statute and its legislative history demonstrates that it limits the FTC's Section 5 regulatory authority).

Section 5's plain language does not authorize patient-information data-security regulation, and Congress has enacted many statutes that, taken together, independently prohibit the FTC from regulating patient-information data-security and strictly cabin its authority to regulate data-security practices in other economic sectors. The FTC does not have the authority to regulate LabMD's patient-information data-security practices. Therefore, the Complaint should be dismissed.

A. Congress Authorized HHS, Not The FTC, To Regulate Patient-Information Data-Security Practices.

Congress has enacted specific legislation, HIPAA and HITECH, setting patient-information data-security standards and delegating to HHS the relevant interpretative and enforcement authority. Consequently, even if Section 5 does authorize the FTC to regulate data-security, which it does not, the Commission lacks legal sanction for the things that it has done to LabMD.

1. Controlling interpretative canons hold the FTC's general Section 5 authority (if any) must yield to the specific patient-information statutes and regulations.

To begin with, the well-known interpretative canon that a general statute must yield to a more specific one applies here. As the Supreme Court recently held:

[6] The Commission has admitted to Congress that this is how Section 5 should be interpreted. *See* FTC, *Policy Statement on Unfairness* 2 (Dec. 17, 1980), appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984).

> The general/specific canon...has full application as well to statutes such as the one here, in which a general authorization and a more limited, specific authorization exist side-by-side. There the canon avoids not contradiction but the superfluity of a specific provision that is swallowed by the general one, "violat[ing] the cardinal rule that, if possible, effect shall be given to every clause and part of a statute."

RadLAX Gateway Hotel, LLC v. Amalgamated Bank, 132 S. Ct. 2065, 2070-71 (2012)(citation omitted).

HIPAA requires LabMD to meet security standards for electronic health information, such as the PI file. HITECH requires HIPAA-regulated entities to provide notice of unsecured breaches of health information in certain circumstances and strengthens protections for such data. Congress vested HHS with exclusive administrative and enforcement authority with respect to HIPAA-covered entities under these laws.[7] *See, e.g.*, 42 U.S.C. § 1320d-2(d)(1)("Security standards for health information"). Recognizing this, the FTC has repeatedly told Congress that HIPAA and its privacy rule are not enforced by the Commission.[8]

[7] Unlike the Commission, HHS has actually promulgated regulations establishing reasonably ascertainable patient-information data-security standards.

[8] For example, in March 2005, Commission Chairwoman Deborah Majoras said that HIPAA is "not enforced by the Commission." *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Statement Before the U.S. Senate, Committee on Banking, Housing, and Urban Affairs*, 109th Cong., 6 (2005). This understanding was reaffirmed before Congress in 2007. *See Protecting the Privacy of the Social Security Number from Identity Theft: Statement Before the Subcommittee on Social Security of the House Committee on Ways and Means*, 110th Cong. 10 (2007)(prepared statement of Joel Winston, FTC). The preambles to HHS's HIPAA rules refer to the single national standard the HIPAA regulations establish. *See* 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000)(Privacy Rule)("This…rule establishes, for the first time, a set of basic national privacy standards and fair information practices…."); 68 Fed. Reg. 8,334, 8,334 (Feb. 20, 2003)(Security Rule)("The purpose of this…rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information."); *see also* U.S. Dep't of Health & Human Servs., *Security 101 for Covered Entities, HIPAA Security Series*, Vol. 2/Paper 1, 3 (2007)("Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry."), *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf (accessed Nov. 3, 2013).

HITECH's plain language confirms Congress's intent that data-security standards for HIPAA-covered entities be regulated exclusively by HHS, not the FTC. HITECH §13422(b)(1) directs HHS, in coordination with the FTC, to study data-security requirements for non-HIPAA-covered entities and determine "which Federal government agency is best equipped to enforce such requirements recommended to be applied to…[non-HIAPA-covered entities]…and a timeframe for implementing regulations based on such findings." Pub L. 111-5 § 13422(b)(1), 123 Stat. 226, 277 (2009); *see also* 42 U.S.C. § 17937 (giving the FTC authority to establish temporary data-breach notification requirements for non-HIPAA-covered entities).

If the Commission already had such authority, HITECH and many other data-security statutes would be superfluous. Indeed, if Congress intended to give the FTC authority to regulate patient-information data-security (or believed that the FTC already had this authority), then it would not have drawn a clear distinction between HIPAA-covered and non-HIPAA-covered entities and specifically given the FTC such limited authority to regulate non-covered entities, for the mention of one thing suggests the exclusion of another.[9] *See, e.g., United States v. Lopez*, 938 F.2d 1293, 1297 (D.C. Cir. 1991); *see Indep. Ins. Agents of Am., Inc. v. Hawke*, 211 F.3d 638, 645 (D.C. Cir. 2000)("[T]he cannons of avoiding surplusage and expressio unius are at their zenith when they apply in tandem."). Clearly, Congress charged HHS, and not the FTC, with regulating LabMD's patient-information data-security practices, and it is inappropriate for the Commission to bulldoze these boundaries. *See* 78 Fed. Reg. at 5,687-5,702.

[9]As HHS recently explained, the "entities operating as HIPAA covered entities and business associates are subject to HHS' and not the FTC's, breach notification rule." 78 Fed. Reg. 5,566, 5,639 (Jan. 25, 2013); *accord* 74 Fed. Reg. 42,962, 42,964-65 (Aug. 25, 2009)("HIPAA-covered entities and entities that engage in activities as business associates of HIPAA-covered entities will be subject only to HHS' rule and not the FTC's rule….").

2. The *Billing* doctrine controls and so the FTC has no authority.

Because there is a "clear repugnancy" between the specific and targeted regulatory enactments of HIPAA and HITECH, on the one hand, and Section 5's general unfairness language, on the other, the later must yield to the former, and so the FTC has no authority over LabMD's patient-information data-security. *See Credit Suisse Sec. LLC v. Billing*, 551 U.S. 264, 275 (2007).

In *Billing*, the Supreme Court held that the regulatory provisions of the securities laws, by implication, precluded the more general antitrust law. Preclusion obtained in that case based on an analysis of (1) the existence of regulatory authority under the securities law to supervise the activities in question; (2) evidence that the responsible regulatory entities exercise that authority; (3) a resulting risk that the specific securities and general antitrust laws, if both applicable, would produce conflicting guidance, requirements, duties, privileges, or standards of conduct; and (4) the possible conflict between the laws with respect to affected practices that lie squarely within an area of financial market activity that the securities laws seek to regulate. *See id.* at 275-76.

HIPAA/HITECH and the FTC's claimed Section 5 authority to regulate patient-information data-security practices are "clearly incompatible," and so *Billing* holds that Section 5 and the FTC must yield. This is because (1) Congress gave HHS specific regulatory authority over patient-information data-security practices; (2) HHS exercises that authority, as evidenced by its repeated promulgation of data-security standards for healthcare providers, *see e.g.* 78 Fed. Reg. 5,566 (Jan. 25, 2013); (3) as demonstrated by this proceeding, there is a risk of conflicting standards of conduct (notably, the FTC agrees that LabMD has not violated HIPAA or HITECH, Trans. 22:10-13); and (4) this possible conflict with Section 5 affects practices that lie squarely within an area of healthcare activity regulated under HIPAA/HITECH. *See supra* notes 4 & 9.

Thus, HIPAA/HITECH preclude application of Section 5 to LabMD's patient-information data-security practices. *See Billing*, 551 U.S. at 275-76.

B. Congress Has Not Given The FTC The Plenary Power To Regulate Data-Security Through Its Section 5 "Unfairness" Authority.

The FTC claims its general Section 5 "unfairness" authority allows it to regulate LabMD's patient-information data-security. However, Congress has never given the Commission such authority and has, in fact, repeatedly made it clear that the FTC's power is very limited in application and very narrow in scope.

1. The FTC's claim of general Section 5 "unfairness" authority to regulate data-security practices is contradicted by Congress's many specific data-security delegations.

The FTC's claim of general Section 5 "unfairness" authority to regulate LabMD and other companies is contradicted by Congress's many specific delegations of data-security authority.

To begin with, when Congress has wanted the FTC to have data-security authority, it has said so. To date, Congress has specifically authorized the Commission to regulate data-security practices in at least three statutes, including the Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley Act (GLBA), and the Children's Online Privacy Protection Act (COPPA).[10] The FTC has argued elsewhere that the FCRA, GLBA, and COPPA merely "enhance FTC authority

[10] The FCRA, 15 U.S.C. § 1681 *et seq.*, as amended by the Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, 111 Stat. 1952 (2003), establishes requirements for the collection, disclosure, and disposal of data collected by consumer reporting agencies and requires the FTC and other agencies to develop rules for financial institutions to reduce the incidence of identity theft. The GLBA, Pub. L. 106-102, 113 Stat. 1338 (1999)(codified 15 U.S.C. §§ 6801-6809), mandates data-security requirements for financial institutions and instructs the FTC and federal banking agencies to establish standards for financial institutions "to protect against unauthorized access to or use of such records or information," 15 U.S.C. § 6801(b)(3). The COPPA, Pub. L. 105-277, 112 Stat. 2681 (1998)(codified 15 U.S.C. § 6501 *et seq.*), requires website operators to establish and maintain reasonable procedures to protect the confidentiality and security of information gathered from children.

with new legal tools," such as "rulemaking and/or civil penalty authority…." Plaintiff's Opposition to Motion to Dismiss, *FTC v. Wyndham Worldwide Corp.*, No. 2:13-cv-01887-ES-SCM, Dkt. No. 110, at 12 (D. N.J. May 20, 2013)(the "FTC Opposition"). But this argument fails, for these statutes explicitly authorize the Commission to set substantive data-security standards. *See* 15 U.S.C. §§ 1681m(e)(1), 6804(a)(1)(C), 6502(b), and to enforce those standards under the FTCA, *see* 15 U.S.C. §§ 1681s(a), 6805(a)(7), 6505(d). If Section 5 generally authorized the FTC to do these things, these provisions would be meaningless exercises, *Rumsfeld v. Forum for Academic & Institutional Rights, Inc.*, 547 U.S. 47, 58 (2006), as "there would have been no reason for Congress to have included" them, *Stone v. INS*, 514 U.S. 386, 397 (1995). The Commission cannot assume that Congress passes purposeless legislation. *Babbitt v. Sweet Home Chapter of Cmtys. for a Great Or.*, 515 U.S. 687, 701 (1995). Therefore, FCRA, GLBA, COPPA, and other narrowly tailored statutes are the only authorities authorizing the FTC to regulate data-security practices of any sort.

At the same time, Congress has enacted numerous other targeted statutes specifically delegating statutory authority over data-security, including HIPAA, HITECH, the Cable Television Consumer Protection and Competition Act, Pub. L. 102-385, 106 Stat. 1460 (1992)(codified at 47 U.S.C. § 521 *et seq*.); the Video Privacy Protection Act, Pub. L. 100-618, 102 Stat. 8195 (1988)(codified at 18 U.S.C. § 2710); Driver's Privacy Protection Act of 1994, Pub. L. 103-322, 106 Stat. 2099 (1994)(codified at18 U.S.C. § 123); and the Computer Fraud Abuse Act of 1986, Pub. L. 99-474, 100 Stat. 1213 (1986)(codified as amended at 18 U.S.C. § 1030 *et seq*.).[11] If the FTC's Section 5 unfairness authority included general, economy-wide authority to regulate data-security, then all of these statutes, creating and delegating regulatory

[11] This list is illustrative, not exhaustive.

authority to HHS and other agencies, would also necessarily be superfluous nullities. The Commission's Section 5 power-grab here therefore offends the rule against attributing redundancy to Congress, *Gutierrez v. Ada*, 528 U.S. 250, 258 (2000), and is at odds with the interpretive canon that no statute should be interpreted in a fashion that renders its parts "inoperative or superfluous." *See Corley v. United States*, 556 U.S. 303, 314 (2009).

2. The Commission's claim of Section 5 "unfairness" authority to regulate data-security economy wide is contrary to congressional intent and to controlling Supreme Court authorities.

As the Commission itself frequently acknowledged—until it recently reversed course without explanation or opportunity for notice and comment from stakeholders, both in violation of the law, *see FCC v. Fox TV Stations, Inc.*, 556 U.S. 502, 514-15 (2009)(an agency must explain policy change)—Section 5 does not give the FTC the authority to regulate data-security practices as "unfair" acts or practices or the authority to require firms to adopt information practice policies.[12] This is why Congress enacted FCRA, GLBA, COPPA, HIPAA, HITECH, and numerous other targeted data-security laws.

[12] For many years, the Commission said its authority over data-security matters was "limited...to ensuring that Web sites follow their stated information practices." *Consumer Privacy on the World Wide Web, Hearing before Subcomm. on Telecomm. of the H. Comm. on Commerce Subcomm. on Telecomm.*, 105th Cong. n.23 (1998)(statement of Robert Pitofsky, Chairman, FTC), *available at* http://www.ftc.gov/os/1998/07/privac98.htm; *see also* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 137 (2008). As a Commission official explained in 2001, "'[t]he agency's jurisdiction is (over) deception….The agency doesn't have the jurisdiction to enforce privacy.'" Jeffrey Benner, *FTC Powerless to Protect Privacy*, Wired (May 31, 2001), http://www.wired.com/politics/security/news/2001/05/44173 (quoting Lee Peeler, former Associate Director of Advertising Practices at the FTC); *accord* FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, 34 (2000)(hereinafter "*2000 Privacy Report*"), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (accessed November 3, 2013); FTC, *Privacy Online: A Report to Congress*, 41 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf ("Commission [generally] lacks authority to require firms to adopt information practice policies….")(accessed Nov. 3, 2013); *see also Protecting Information Security and Preventing Identity Theft, Hearing before Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census of H. Comm. on Gov't Reform*,

The Commission's lack of power to regulate data security through its general Section 5 "unfairness" authority also explains why the Commission has, for over a decade, asked Congress for legislation authorizing it to do what it has done to LabMD.[13] In May 2012, John Leibowitz, then-Commission Chairman, asked once more for the power to enforce data-security measures.[14] Yet, Congress has consistently refused, over a period of many years, to give the Commission what it wants,[15] considering and rejecting several proposals to give the

---

108th Cong. 7 (statement of Orson Swindle)(2004)("To date, the Commission's security cases have been based on its authority to prevent deceptive practices."), *available at* http://www.ftc.gov/os/2004/09/040922infosecidthefttest.pdf (accessed Nov. 3, 2013).

[13] *See, e.g.*, *2000 Privacy Report* at 36-37 (asking Congress to enact legislation requiring websites to "take reasonable steps to protect the security of the information they collect" and providing "the authority to promulgate more detailed standards"); *see also Data Security: Hearing Before the H. Comm. on Energy & Commerce*, 112th Cong. 11 (2011)(statement of David C. Vladeck, Director of the Bureau of Consumer Protection, FTC)("[T]he Commission reiterates its support for federal legislation that would…impose data security standards on companies…."); *Data Security: Hearing Before the H. Comm. on Energy & Commerce*, 112th Cong. 11 (2011)(statement of Edith Ramirez, Commissioner, FTC)(same); *Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act: Hearing Before H. Comm. on Energy & Commerce*, 111th Cong. 12 (2009)(prepared statement of Eileen Harrington, FTC)(The FTC "has recommended legislation requiring all companies that hold sensitive consumer data to take reasonable measures to safeguard it.").

[14] *Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission, Hearing Before S. Comm. on Commerce, Science, and Transportation* 112th Cong. 1-2 (2012)(statement of John Leibowitz, Chairman, FTC). Leibowitz noted in a footnote that then-Commissioner Thomas Rosch believed that "in contravention of our promises to Congress, [the Commission's] privacy framework is based on an improper reading of our consumer protection 'unfairness' doctrine…." *Id.* at 3 n.2. Indeed, even the Commission's 2008 Resolution did not claim that the Commission can regulate data-security practices under a pure unfairness theory. *See* Resolution Directing Use of Compulsory Process In Nonpublic Investigation of Acts and Practices Related to Consumer Privacy And/Or Data Security, File No. P954807 (Jan. 3, 2008)(authorizing an investigation into "deceptive or unfair acts or practices related to consumer privacy and/or data security…in violation of Section 5"). The Complaint has not alleged that LabMD engaged in deceptive practices. *See* Compl. ¶¶22-23.

[15] *See, e.g.*, Personal Data Privacy and Security Act of 2011, S. 1151, 112th Cong. (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Cong. (2011); Data Breach Notification Act of 2011, S.1408, 112th Cong. (2011); Data Security Act of 2011, S.1434, 112th Cong. (2011); Personal Data Protection and Breach Accountability Act of 2011,

Commission the general authority to regulate data security. *Cf. Brown & Williamson*, 529 U.S. at 147. In other words, Congress has ratified the Commission's previous position that it lacks general jurisdiction to regulate data-security practices under Section 5.[16] *See id.* at 156.

If Congress had intended for the Commission's Section 5 "unfairness" authority to include patient-information data-security practices, it could have said so in the Federal Trade Commission Act Amendments of 1994, codified at 15 U.S.C. § 45(n). Instead, due to a long history of Commission abuses, Congress stripped it of the authority "to declare unlawful an act or practice" under Section 5 unless "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." *Id.*; *see* Statement by Director of Consumer Protection Howard Beales, *FTC's Use of Unfairness Authority*, *available at* http://www.ftc.gov/speeches/beales/unfair0603.shtm (accessed Nov. 3, 2013). Congress also said that public policy concerns are not a primary basis for the exercise of jurisdiction, 15 U.S.C. § 45(n), thereby legislatively overruling prior judicial Section 5 interpretations. *See, e.g., Atl. Ref. Co. v. FTC*, 381 U.S. 357, 369 (1965), *superseded by statute.*

At the time, the Commission did not claim Section 5 "unfairness" authority to regulate patient-information (or any other) data-security practices. But now it has changed its tune and

---

S. 1535, 112th Cong. (2011); Data Accountability and Trust Act, H.R 1707, 112th Cong. (2011); Data Accountability and Trust Act of 2011, H.R 1841, 112th Cong. (2011); SAFE Data Act, H.R. 2577, 112th Cong. (2011).

[16] The Commission's extralegal approach to data-security regulation also violates the core principles espoused in Executive Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013), which directs the Department of Commerce (not the Commission) to identify specific data-security practices through the notice-and-comment process, *see id.* § 7; *see also* Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, at 29 n.33 (Feb. 2012)("[T]he FTC does not currently have authority to enforce Section 5…against certain corporations that operate for profit…."), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

grabs for massive plenary powers over the entire economy. Yet, Section 5 does not and was not intended to give the Commission authority to do this. Congress does not hide massive regulatory schemes in statutory mouseholes. *Whitman v. Am. Trucking Ass'ns., Inc*., 531 U.S. 457, 468 (2001); *see also Brown & Williamson*, 529 U.S. at 160. This holds true *a fortiori* where, as here, the Commission claims its broad authority from vague general statutory terms in the face of both an amended Section 5 that was designed to rein in the Commission's abuse of its "unfairness" authority and a raft of specific, targeted data-security statutes, including HIPAA and HITECH.

Simple "common sense as to the manner in which Congress is likely to delegate a policy decision of such economic and political magnitude," *Brown & Williamson*, 529 U.S. at 133, as general regulatory authority over the data-security practices of all private businesses in the United States reinforces the conclusion that the FTC lacks the authority to regulate the acts or practices alleged in the Complaint. As in *Brown & Williamson*, to conclude that Section 5 gives the FTC jurisdiction over data-security requires not only an "extremely strained understanding" of a vague term ("unfairness") in the FTCA, *cf. id.* at 160-61 (discussing FDA's misinterpretation of the word "safety" in the Food, Drug, and Cosmetic Act), "but also ignor[ing] the plain implication of Congress' subsequent…[data-security]-specific legislation," *id.* at 160. There, as here, Congress could not have intended to grant unfettered power to prescribe data-security standards for private companies, a topic of intense debate with immense economic consequences, to the Commission "in so cryptic a fashion." *Id.* at 160.

In *Brown & Williamson* the Supreme Court rejected the FDA's overreaching. *See id.* at 125. There, as here, the agency pestered Congress to pass legislation expanding its authority but Congress instead chose a more targeted, narrowly tailored regulatory scheme. *See id*. at 153-

54, 156, 158 (Congress enacted numerous tobacco-specific statutes incrementally expanding regulatory authority). Thus, *Brown & Williamson* controls and requires rejection of the Commission's claimed Section 5 "unfairness" authority to regulate LabMD's patient-information data-security practices.

C. *ABA v. FTC* Stands For Dismissal.

The case of *ABA v. FTC*, 430 F.3d at 470-71, stands for dismissal.

There, the D.C. Circuit denied the FTC's attempted power-grab to regulate attorneys under the GLBA, ruling that Congress had not directly and plainly granted the Commission the authority to regulate and rejecting the FTC's claim that statutory gap-filling justified a massive expansion of its authority. *See id.* at 470-71. The court said that Congress's decision not to specifically authorize attorney regulation in the GLBA "makes an exceptionally poor fit with the FTC's apparent decision that Congress, after centuries of not doing so, has suddenly decided to regulate the practice of law." *Id*. at 470. It also said that attorney regulation was historically the province of the states and that federal law "'may not be interpreted to reach into areas of State sovereignty unless the language of the federal law compels the intrusion.'" *Id.* at 472 (citation omitted).

ABA's reasoning applies with equal force here. First, there is nothing in Section 5 explicitly authorizing the FTC to directly regulate patient-information data-security practices. Instead, as in *ABA*, the Commission is simply grabbing power to "fill in" what it perceives to be a regulatory gap. But Congress has already filled the patient-information data-security regulatory "gap" through HIPAA and HITECH, and it is not for the FTC to second-guess Congress. The FTC's assault on LabMD is contrary to the administrative structure Congress has constructed for patient-information data-security and entirely illegitimate. *See id.* at 470-71; *see also Brown & Williamson*, 529 U.S. at 160.

Second, Congress has generally left healthcare-provider data-security regulation to the states. This is because regulation of privacy and healthcare is traditionally a matter of local concern.[17] *See* 65 Fed. Reg. at 82,463 ("Rules requiring the protection of health privacy in the United States have been enacted primarily by the states."); *see also Hill v. Colo.*, 530 U.S. 703, 715-18 (2000)(upholding statute protecting patient privacy as valid exercise of state's traditional police power to protect health and public safety); *Hillsborough Cnty. v. Automated Med. Laboratories*, Inc., 471 U.S. 707, 719 (1985)(The "regulation of health and safety matters is primarily, and historically, a matter of local concern."). In those cases where Congress has determined federal regulation of patient-information data-security practices is appropriate, it has explicitly said so. *See, e.g.*, 42 U.S.C. § 1320d-2(d)(1). Because Section 5 does not contain a clear and manifest statement from Congress to authorize the Commission's intrusion into patient-information data-security, its brazen fabrication of authority and grab for power should be rebuffed. *See ABA*, 430 F.3d at 472.

[17] Pub. L. No. 104-191, 110 Stat. 1936, § 264(c)(2) states that HIPAA regulations "shall not supersede a [more robust] contrary provision of State law," consistent with traditional state regulation of public health and welfare. *See Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485 (1996); *see also* John R. Christiansen, *Legal Speed Bumps on the Road to Health Information Exchange*, J. HEALTH & LIFE SCI. L., January 2008, at 1, 1 ("Before HIPAA, state privacy and confidentiality laws were almost the exclusive source of information protection requirements. HIPAA still defers to state laws that are more protective of PHI…."); Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies And Laws*, 19 ALB. L. J. SCI. & TECH. 91, 104-105 & n.66 (2009)(noting that "all but six states and the District of Columbia have passed legislation requiring entities, particularly businesses that maintain computerized personal information…, to notify those residents if their personal information has been disclosed through a data breach" and listing statutes).

II. THE COMMISSION HAS FAILED TO GIVE FAIR NOTICE OF WHAT DATA-SECURITY PRACTICES IT BELIEVES SECTION 5 FORBIDS OR REQUIRES THEREBY VIOLATING LABMD'S DUE PROCESS RIGHTS.

The Commission has refused to publish data-security regulations, guidance, or standards explaining what is either forbidden or required by Section 5. Therefore, it has denied LabMD and others similarly situated constitutionally required fair notice, engaged in prohibited *ex post facto* enforcement, and, through this action, violated LabMD's due process rights. *See Satellite Broad. Co. v. FCC*, 824 F.2d 1, 3 (D.C. Cir. 1987)(traditional concepts of due process incorporated into administrative law preclude agencies from penalizing private parties for violating rules without first providing adequate notice of their substance); *Trinity Broad. of Fla., Inc. v. FCC*, 211 F.3d 618, 632 (D.C. Cir. 2000)(where the regulations and other policy statements are unclear, where the petitioner's interpretation is reasonable, and where the agency itself struggles to provide a definitive reading of the regulatory requirements, a regulated party is not "on notice" and may not be punished).

A. Due Process Requires Fair *Ex Ante* Warning of Prohibited or Required Conduct.

"A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *FCC v. Fox TV Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012). Administrative law has thoroughly incorporated this constitutional fair notice requirement to limit agencies' ability to regulate past conduct through after-the-fact enforcement actions. *See Satellite Broad. Co. v. FCC*, 824 F.2d at 3. Where, as here, a party first receives notice of a purportedly proscribed activity through an enforcement action, due process rights are violated. *See, e.g., United States v. Chrysler Corp.*, 158 F.3d 1350, 1355 (D.C. Cir. 1998)(due process requires fair notice of standard before company could be ordered to recall vehicles for alleged noncompliance with standard).

B. The Commission Has Denied LabMD Fair Notice.

The test for constitutionally adequate notice is whether by reviewing the regulations and other public statements issued by the agency, a regulated party acting in good faith would be able to identify, with ascertainable certainty, the standards to which the agency expects parties to conform. *Trinity Broad.*, 211 F.3d at 632. The Commission "has the responsibility to state with ascertainable certainty" what standards third parties must follow. *Gates & Fox Co. v. OSHRC*, 790 F.2d 154, 156 (D.C. Cir. 1986)(citation omitted). It has failed to do so in this case.

The Commission is authorized to prescribe regulations specifically defining unfair acts or practices. 15 U.S.C. § 57a(a)(1). However, Section 5 independently bars the Commission from attempting to enforce consent orders against non-parties. 15 U.S.C. § 45(m)(1)(B). And the APA categorically prohibits federal agencies from creating legislative rules and substantive standards through mechanisms other than formal or notice-and-comment rulemaking. Consequently, the Commission cannot point to any legally-binding data-security standards, and so its attack against LabMD violates the company's due process rights.

1. The Commission has wrongfully failed to provide *ex ante* notice through regulations.

Section 5's general prohibition of "unfair" acts or practices is constitutionally too vague to provide adequate *ex ante* notice of the patient-information data-security practices that it purports to forbid or require. *See Connally v. Gen. Constr. Co.*, 269 U.S. 385, 391 (1926)(statute that either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application violates due process); *Trinity Broad.*, 211 F.3d at 632. Furthermore, the FTC admits that it has not prescribed regulations or legislative rules under Section 5 establishing patient-information (or any other) data-security standards that have the force of law. Trans. 21:11-22:13.

The FTC's refusal to issue regulations is wrongful and makes no sense. It has in the past issued data-security regulations after notice-and-comment rulemaking in a number of areas. For example, 16 C.F.R. Pt. 314 sets forth specific standards under the GLBA "for developing, implementing, and maintaining reasonable" technical safeguards to protect consumer information. *See* 16 C.F.R. § 314.1. Also, 16 C.F.R. Pt. 682 implements the FCRA by articulating specific guidelines regarding the proper destruction of consumer information. *See* 16 C.F.R. § 682.3. Therefore, there is no reason the FTC could not have announced similar *ex ante* rules here, other than the FTC's admission that it prefers the "regulatory flexibility" of employing a vague standard such as "reasonableness." *See* FTC Opposition at 21-22; Trans. 21:11-25. But unchecked discretion is not a virtue of the FTC's current interpretation of its Section 5 "unfairness" authority, and it is for that very reason that such a regime cannot be lawful. *See City of Chicago v. Morales*, 527 U.S. 41, 63-64 (1999)(boundless enforcement discretion violates due process); *Connally*, 269 U.S. at 391.

2. <u>The FTC's alleged "standards" are legally meaningless.</u>

The FTC has claimed that its "public statements," "educational materials," and "industry guidance pieces" establish standards and provide LabMD and others similarly situated with notice of the data-security practices they must keep to avoid Section 5 "unfairness" liability. Trans. 9:23-10:3. This claim is untenable for several reasons.

First, general statements of policy are prospective and do not create obligations enforceable against third parties like LabMD. *See Am. Bus. Ass'n. v. United States*, 627 F.2d 525, 529 (D.C. Cir. 1980)("The agency cannot apply or rely upon a general statement of policy as law because a…policy statement announces the agency's tentative intentions for the future." (citation omitted)); *Wilderness Soc'y v. Norton*, 434 F.3d 584, 595-96 (D.C. Cir. 2006)(in holding agency manuals to be nonbinding, the court said that "it is particularly noteworthy that

NPS did not issue its management policies through notice and comment rulemaking under 5 U.S.C. § 553" because failure to do so is evidence that the material in question was not supposed to be a rule binding regulated companies' conduct).

Second, if the FTC truly considers "public statements," "educational materials," and "industry guidance pieces" to be enforceable standards, then it necessarily concedes an APA violation. The APA requires agencies to "publish in the Federal Register for the guidance of the public…substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency…." 5 U.S.C. § 552(a)(1)(D). It further provides that except to the extent "that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published." 5 U.S.C. § 552(a)(1).

Therefore, the Internet postings of "Guides for Business," links to SANS Institute and NIST publications, and similar materials on the Commission's official website do not replace Federal Register publication.[18] The D.C. Circuit has never found that Internet notice is an acceptable substitute for publication in the Federal Register, and has affirmatively refused to do so. *Util. Solid Waste Activities Grp. v. EPA*, 236 F.3d 749, 754 (D.C. Cir. 2001). Here, the Complaint does not even allege that LabMD had actual notice of any of these sources. Thus, the FTC has breached its statutory duty.[19]

[18] Curiously, other Commission "business guides" that have been posted on the Internet have also been published in the Federal Register. *See, e.g.*, Guides for Jewelry, Precious Metals, and Pewter Industries, 16 C.F.R. § 23 (2013), *available at* http://www.ftc.gov/os/2012/06/120622jewelryguidesfrn.pdf.

[19] The FTC claims that NIST publications allegedly setting forth "principles" about what they call the "general approach" of "[d]efense in depth," Trans. 11:18-24, establish ascertainable standards. That claim is contradicted by NIST itself. A NIST publication

Third, the FTC cannot regulate by consent order. *See Gen. Elec. Co. v. EPA*, 290 F.3d 377, 382-83 (D.C. Cir. 2002)(holding that an agency guidance document that imposes binding duties and obligations violates the APA). Consent orders "do not establish illegal conduct," *Intergraph Corp. v. Intel Corp.*, 253 F.3d 695, 698 (Fed. Cir. 2001), and are "only binding upon the parties to the agreement," *Altria Grp., Inc. v. Good*, 555 U.S. 70, 89 n.13 (2008). They do not restrict the FTC's discretion in future actions and therefore do not provide the fair notice that due process requires. *See Morales*, 527 U.S. at 63-64.

Furthermore, Congress specifically barred the Commission from binding third parties by consent order, prohibiting the FTC from enforcing a "consent order" against anyone who is not a party to it.[20] 15 U.S.C. § 45(m)(2); *see Good v. Altria Group, Inc.*, 501 F.3d 29, 53 (1st Cir.

---

addressing the HIPAA Security Rule states: "This publication is intended as general guidance only…*and is not intended to be, nor should it be construed or relied upon as legal advice or guidance to nonfederal entities or persons.* This document does not modify…[]HIPAA[] or any other federal law or regulation." Scholl et al., *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, NIST Special Pub. 800-66 Revision 1, at iv (2008)(emphasis added). Another NIST publication regarding computer security that the FTC may cite specifically disclaims any intent to establish standards: "*The purpose of this handbook is not to specify requirements*…." *An Introduction to Computer Security: The NIST Handbook*, NIST Special Pub. 800-12, at 3 (1995)(emphasis added). That argument therefore fails.

The FTC also argues that the SANS Institute establishes data-security standards that LabMD should have complied with. That, too, is wrong. The SANS Institute is merely a "cooperative research and education organization." SANS, About, http://www.sans.org/about/. It does not have the authority to prescribe legislative rules or otherwise establish binding standards. Voluntary industry standards are not law and do not purport to reveal what the Commission (or any other entity) believes Section 5 to require. *See, e.g., Romero v. Buhimschi*, 2007 U.S. Dist. LEXIS 73024, at *11 (E.D. Mich. 2007)(illustrating proposition that voluntary adoption of private standards of conduct does not create legal duty). Private standards cannot provide the fair notice the Commission has refused to give.

[20] The FTC may assert that consent orders in *other* data-security cases establish reasonably ascertainable standards. *See* FTC Opposition at 19. But, as the Commission has admitted, *see id.*, its prior consent orders are not "controlling precedent for later Commission action" and do not in any way limit the Commission's enforcement powers. *Beatrice Foods Co. v. FTC*, 540 F.2d 303, 312 (7th Cir. 1976). Even if Commission consent orders involving data-security practices could provide notice, which they cannot, Commission consent orders made

2007)(The FTCA "specifically provides that the Commission cannot enforce them against non-parties.").

Finally, none of the alleged standards cited by the FTC, whether NIST and SANS Institute publications, the Commission's patchwork-quilt of nonbinding consent orders (most of which, unlike this matter, involved allegations of deception), or general "Guides for Businesses" and "Consumer Alerts" purport to establish specific patient-information data-security standards that businesses "shall" or "must" abide by. Instead, these alleged sources of data-security standards are couched in, at best, precatory language: "may," "best practices," "recommendations," and the like.[21]

---

publicly available for the first time years after LabMD's alleged "security incidents" cannot give LabMD constitutionally adequate *ex ante* warning. *See, e.g.*, FTC, EPN, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 77 Fed. Reg. 35,387 (June 13, 2012); FTC, Franklin Budget Car Sales, Inc.; Analysis of Proposed Consent Order to Aid Public Comment, 77 Fed. Reg. 35,391 (June 13, 2012).

[21] The FTC may dismiss LabMD's arguments by claiming, as the Commission has elsewhere, that "[LabMD] may argue that it did not know *which* standard it was supposed to follow. This argument misses the point." FTC Opposition at 18 n.5 (emphasis in original). But that is one of LabMD's core points, for "baffling and inconsistent" rules do not give fair notice. *Satellite Broad.*, 824 F.2d at 2-4. Also, the FTC may argue that its Internet postings such as "Protecting Personal Information: A Guide for Business (2007), http://business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf (hereinafter "PPI Guide"), are enough. *See* FTC Opposition at 18-19. But this "Guide for Business" states that "there's no one-size-fits-all approach to data security, and what's right for you depends on the nature of your business and the kind of information you collect from your customers." PPI Guide at 23. This is hardly "fair notice" of anything at all.

In 2011, the Commission also posted on the Internet a document entitled "Peer-to-Peer File Sharing: A Guide for Business." But the Complaint's allegations regarding a "P2P file sharing application" occurred in 2008, three years *before* this document was posted on the Internet. Moreover, it does not cite Section 5 or *any* regulations or binding standards. It does not make clear what, if anything, businesses are legally required or prohibited from doing, e.g., "[w]hether you decide to ban P2P file sharing programs on your network or allow them, it's important to create a policy and take the appropriate steps to implement and enforce it…." FTC, *Peer-to-Peer File Sharing: A Guide for Business* 3 (2011), *available at* http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business.pdf. Simply put, this document contains nothing resembling an intelligible, much less enforceable, binding legal standard.

Consequently, the FTC has denied LabMD and others similarly situated the fair notice they are entitled to as a matter of constitutional right. *Gates & Fox Co.*, 790 F.2d at 156.

III. THE ACTS OR PRACTICES ALLEGED IN THE COMPLAINT DO NOT AFFECT INTERSTATE COMMERCE.

FTCA Section 4 defines "commerce" as commerce "among" or "between" states. 15 U.S.C. § 44; *see FTC v. Buntes Bros., Inc.*, 312 U.S. 349, 351-55 (1941). Section 5 allows the Commission to regulate "unfair…acts or practices in or affecting commerce" that have actually caused substantial (usually monetary) harm. 15 U.S.C. § 45(a)(1); *In the Matter of Int'l Harvester*, 104 F.T.C. 949, at 248 (1984)(unfairness cases usually involve "actual and completed harms," often monetary but sometimes health and safety). LabMD's principal place of business, where all of the alleged acts or practices allegedly occurred, is located in Georgia. Compl. ¶1. All of its servers and its computer network are located in Georgia. None of the alleged FTCA violations allegedly occurred outside of Georgia and there are no allegations of monetary loss or other actual harm. Therefore, dismissal with prejudice is appropriate.

IV. THE COMPLAINT DOES NOT COMPLY WITH THE COMMISSION'S PLEADING REQUIREMENTS.

Although the Commission's "unfairness" claim hinges on proving that LabMD's data-security practices were not "industry standard" or "commercially reasonable," the Complaint contains no allegations at all explaining what data-security practices were "standard" in the medical industry between 2008 and 2012, when the alleged "Security Incidents" occurred, or how LabMD's practices fell short of this unspecified benchmark. Further, the addition of technical jargon surrounding the Commission's claim of unreasonableness does not change that the Complaint's allegations are nothing more than inadequate "legal conclusion[s] couched as…factual allegation[s]." *Twombly*, 550 U.S. at 555 (citation omitted).

The FTC does not dispute that LabMD complied with HIPAA and HITECH. Trans. 22:10-13. Moreover, the Complaint fails to allege any actual, completed economic harms or threats to health or safety. Therefore, the Complaint does not state a plausible claim for relief and should thus be dismissed.

V. THIS MATTER SHOULD BE STAYED PENDING DISPOSITION OF THIS MOTION.

Under its Rules of Practice, the Commission has the discretion to stay this matter pending its resolution of this Motion. Rule 3.22(b), 16 C.F.R. § 3.22(b)(Commission authorized to stay proceedings); Rule 3.21(c)(1), 16 C.F.R. § 3.21(c)(1)(Commission may continue evidentiary hearing for good cause); Rule 3.41(b), 16 C.F.R. § 3.41(b)(same). The Commission should exercise its discretion here and grant LabMD's request for a stay pending the resolution of its Motion to Dismiss.

In support of its action against LabMD, the FTC has undertaken extensive and abusive discovery. Notwithstanding years of investigation, multiple CIDs, depositions of LabMD's principals, and the production of thousands of pages of documents, the FTC has served burdensome, repetitive, and oppressive discovery requests that would not be allowed under the Federal Rules of Civil Procedure. For example, in a three-hour period on October 24, 2013, the FTC noticed twenty (20) depositions to be taken in various parts of the country, all of which were initially scheduled at the same time on the same day;[22] served eleven (11) subpoenas duces tecum; and served the FTC's First Set of Requests for Production and Interrogatories.

[22] In recognition of the burden and expense of depositions for private litigants that, unlike large federal agencies, do not have unlimited resources, in federal court, leave of court is (quite sensibly) required if a party wishes to take more than ten depositions. Fed. R. Civ. P. 30(a)(2)(A)(i). For that matter, Complaint Counsel has already deposed one of the named deponents during its investigation of LabMD. In federal court, leave of court would also be required for this, for obvious reasons. Fed. R. Civ. P. 30(a)(2)(A)(ii).

LabMD has moved for a protective order. However, it is clear that the FTC's intentions include the punishment of LabMD and subjecting it to ruinous litigation costs, perhaps to chill others from contesting Commission overreach,[23] and all at taxpayer expense. Forcing LabMD to litigate a case that the Commission does not even have jurisdiction to bring is inherently unjust and violates its due process rights. Therefore, a stay of the administrative proceedings until LabMD's Motion to Dismiss is finally resolved would be appropriate.

CONCLUSION

For the foregoing reasons, LabMD respectfully requests that the Commission GRANT its Motion to Dismiss and ORDER that the Complaint be dismissed with prejudice. LabMD further requests that the Commission GRANT its Motion for a Stay of Administrative Proceedings pending the disposition of its Motion to Dismiss.

[23] Notably, the Complaint (along with a FTC press release making disparaging claims about LabMD) was issued shortly before publication of LabMD's CEO's book, *The Devil Inside the Beltway*, in which he exercises his First Amendment right to speak candidly about a matter of public concern and criticizes Complaint Counsels' actions and the Commission's treatment of LabMD in great detail. Complaint Counsels' burdensome and oppressive discovery requests—which run afoul of norms of conduct that obtain in Article III courts and *flagrantly* violate Fed. R. Civ. P. 30(a)(2)(A)'s limits on depositions—followed shortly after the book's publication. The First Amendment prohibits government agencies from retaliating against private citizens for engaging in constitutionally protected speech by bringing baseless enforcement actions. *See Trudeau v. FTC*, 456 F.3d 178, 190-91 nn.22-23 (D.C. Cir. 2006).

Respectfully submitted,

/s/ Reed D. Rubinstein
Reed D. Rubinstein, Partner
D.C. Bar No. 440153
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
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
Admitted only in Maryland.
Practice limited to cases in federal court and
administrative proceedings before federal agencies.

Dated: November 12, 2013

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	)	**DOCKET NO. 9357**
LabMD, Inc., a corporation.	)	**PUBLIC**

[PROPOSED] ORDER GRANTING RESPONDENT LABMD, INC.'S MOTION TO DISMISS COMPLAINT WITH PREJUDICE

This matter came before the Commission on November 12, 2013, upon a Motion to Dismiss the Complaint with Prejudice ("Motion") filed by Respondent LabMD, Inc. ("LabMD") pursuant to Commission Rule 3.22(a), 16 C.F.R. §3.22(a), for an Order dismissing the Federal Trade Commission's ("FTC") Complaint with prejudice. Having considered LabMD's Motion and all supporting and opposition papers, and good cause appearing, it is hereby ORDERED that the FTC's Complaint is DISMISSED with prejudice.

ORDERED:

_____
Edith Ramirez, Chairwoman
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright
Date: Commissioners

CERTIFICATE OF SERVICE

I hereby certify that on November 12, 2013, I filed the foregoing document electronically using the FTC's E-Filing System, which will send notification of such filing to:

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

I certify that I delivered via first-class mail twelve paper copies of the foregoing document to the following address: Document Processing Section, Room H-113, Headquarters Building, 600 Pennsylvania Avenue, N.W., Washington, D.C. 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, Esq.
Megan Cox, Esq.
Margaret Lassack, Esq.
Ryan Mehm, Esq.
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave., N.W.
Mail Stop NJ-8122
Washington, D.C. 20580

CERTIFICATE OF ELECTRONIC FILING

I certify that the electronic copy sent 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 12, 2013

By: _____
Michael D. Pepson

EXHIBIT

20

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FEDERAL TRADE COMMISSION, **Petitioner,** **v.** **LABMD, INC., and MICHAEL J. DAUGHERTY,** **Respondents.**	**1:12-cv-3005-WSD**

OPINION AND ORDER

This matter is before the Court on the Federal Trade Commission's ("FTC," "Commission," or "Petitioner") "Petition of the Federal Trade Commission for an Order to Enforce Civil Investigative Demands" ("Petition") [1].

I. BACKGROUND

On January 3, 2008, the FTC issued a "Resolution Directing Use of Compulsory Process in Nonpublic Investigation of Acts and Practices Related to Consumer Privacy and/or Data Security" (the "2008 Resolution"). (Ex. 2 to Pet. at 3).

The 2008 Resolution authorizes the use of the FTC's compulsory process powers, for a period of five (5) years from its issuance, "[t]o determine whether

unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act [("FTCA")], 15 U.S.C. § 45, as amended." (Id.).

In 2009, the FTC learned that personally-identifiable and sensitive health information belonging to consumers was publically available on peer-to-peer ("P2P") file sharing networks. (Pet. ¶ 6). The FTC undertook a further "inquiry to determine whether disclosures of consumers' sensitive personal information were attributable to failures to employ reasonable data security measures in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), or whether they violated any other statutes or regulations enforced by the Commission." (Id. ¶ 7). The FTC issued Civil Investigative Demands ("CIDs"), pursuant to the 2008 Resolution, to various entities to "obtain copies of electronic files that were located on P2P networks and that contain sensitive information." (Id. ¶ 8). In response to its CIDs, the FTC obtained a spreadsheet (the "1,718 File") that contained information about 9,000 LabMD, Inc. ("LabMD") customers, to include names, Social Security numbers, dates of birth, and personal health insurance information. (Id.).

In 2010, after reviewing the 1,718 File and consulting with law enforcement agencies, the FTC issued a request for information to LabMD in the form of a

"voluntary access request." (Id. ¶ 9). The voluntary access request sought information that would help the FTC determine if LabMD "had violated laws enforced by the Commission by failing to use reasonable and appropriate security measures to safeguard sensitive information." (Id.). LabMD responded to the voluntary access request, but the FTC was dissatisfied with the scope of materials and information that were provided. (Id. ¶ 10).

On December 21, 2011, the FTC issued CIDs to LabMD and its owner and president, Michael J. Daugherty ("Daugherty," collectively "Respondents"), to obtain information it believed it needed to complete its investigation into Respondents' data security policies and practices. (Id. ¶¶ 10-11). The CIDs demanded that: (1) "Daugherty and one or more representatives of LabMD . . . appear and testify at investigational hearings with FTC staff;" (2) "LabMD and Mr. Daugherty . . . respond to a limited set of interrogatories;" (3) "LabMD . . . respond to a single request for documents related to its data security practices that had not already been produced to the Commission in response to the voluntary access requests;" (4) "LabMD and Mr. Daugherty . . . provide interrogatory responses and documents by January 13, 2012, and schedule the investigational hearings for January 23, 2012;" and, (5) LabMD and Daugherty "certify that they had complied with the CID requirements." (Pet. ¶ 11; Ex. 2 to Pet.; Ex. 3 to Pet.).

Between January and June 2012, Respondents sought to limit or quash the CIDs through the administrative appeal process established by the Code of Federal Regulations and Federal Trade Commission Rules. (Pet. ¶¶ 12-15).

On June 21, 2012, Respondents' administrative remedies in challenging the CIDs were exhausted when the FTC denied Respondents' administrative petition to limit or quash the CIDs. (Id. ¶¶ 14-15).

On June 25, 2012, the FTC staff contacted Respondents to discuss their compliance with the CIDs. (Id. ¶ 16). On June 29, 2012, Respondents replied and restated their objections to the CIDs. (Id.).

On August 29, 2012, after Respondents failed to comply with the CIDs, the FTC filed its Petition in this Court seeking an order requiring Respondents to comply with CIDs issued to them on December 21, 2011, pursuant to the FTC's authority under 15 U.S.C. §§ 46, 57b-1 of the FTCA and the 2008 Resolution. (Id. at 1-4). In its Petition, the FTC alleges that the "[R]espondents' failure to comply with the CIDs greatly impedes the Commission's ongoing investigation [into breaches of consumers' sensitive personal information], and prevents the Commission from completing its investigation in a timely manner." (Id. at 9).

On September 5, 2012, the Court ordered: (i) Petitioner to serve Respondents with its Petition; (ii) required Respondents to show cause at a hearing

on September 19, 2012, regarding why the CIDs should not be enforced; and, (iii) directed Respondents to file a pleading "stating their legal and factual support for failing to comply with the FTC's CIDs and explaining why an order should not issue from this Court requiring compliance with the CIDs." (Order of Sept. 5, 2012, [3] at 2-3).

On September 19, 2012, after receiving briefing by the parties, the Court held the show cause hearing and heard argument from the parties. Following the hearing, the Court ordered the FTC to file a supplemental pleading addressing the following questions:

> 1. In a proceeding to enforce an investigative subpoena, what is the FTC required to show to meet the requirement that the subpoena is issued in an inquiry that is within the authority of the agency?
>
> 2. Does the 'plausible' argument standard set out in E.E.O.C. v. Kloster Cruise, Ltd., 939 F.2d 920, 922 (11th Cir. 1991) apply to FTC enforcement actions?
>
> 3. How does the FTC meet the "within the authority of the agency" standard in this case?
>
> 4. What impact, if any, does the Federal Trade Commission's June 21, 2012, decision have on this Court's consideration of the "within the authority of the agency" showing required in this case?
>
> 5. Did LabMD have a means of challenging the Commission's June 21, 2012 decision that the information security investigative inquiry here is within its authority under Section

> 45 and, if so, does that impact the ability of LabMD to raise the issue in this enforcement proceeding?

On September 24, 2012, the FTC filed its supplemental pleading [20]. On September 28, and October 2, 2012, Respondents and the FTC filed a response and reply, respectively [21, 22].

II. DISCUSSION

A. Standard for enforcement of an administrative subpoena

"It is well-settled that the role of a district court in a proceeding to enforce an administrative subpoena is sharply limited; inquiry is appropriate only into whether the evidence sought is material and relevant to a lawful purpose of the agency." Kloster Cruise, 939 F.2d 920, 922 (11th Cir. 1991); see also United States v. Feaster, 376 F.2d 147, 149 (5th Cir. 1967) ("In subpoena cases the Supreme Court has rejected claims that the court must satisfy itself that probable cause exists for the agency's contention that the subject of the subpoena is covered by the statute; the only judicial inquiry to be made in enforcing an agency subpoena is whether the evidence sought is 'plainly incompetent or irrelevant to any lawful purpose' of the agency."); Tobin v. Banks & Rumbaugh, 201 F.2d 223, 224 (5th Cir. 1953) ("[I]n the absence of a clear showing of unreasonableness or gross abuse of the administrative investigative function, the Courts will not interfere with an investigation 'merely in order to render an anticipatory judgment

on the merits.'"). In other words, "a subpoena enforcement proceeding is not the proper forum in which to litigate the question of coverage under a particular statute" and "[t]he agency need not make a conclusive showing of jurisdiction to justify enforcement of the subpoena." Kloster Cruise, 939 F.2d at 922 (citations omitted).[1]

Two inquiries related to the validity of a subpoena issued by a governmental agency are appropriate to be addressed in a subpoena enforcement proceeding: (1) Whether the agency makes a "plausible argument in support of its assertion of jurisdiction"; and (2) Whether the information sought by the subpoena is "plainly incompetent or irrelevant to any lawful purpose [of the FTC]." Id.; see also Ken Roberts Co., 276 F.3d at 587 ("enforcement of an agency's investigatory subpoena will be denied only when there is 'a patent lack of jurisdiction' in an agency to regulate or to investigate"); United States v. Sturm, Ruger & Co., 84 F.3d 1, 5-6 (1st Cir. 1996) (citing Kloster Cruise, 939 F.2d at 923) ("As long as the agency's assertion of authority is not obviously apocryphal, a procedurally sound subpoena

[1] "[C]ourts of appeals have consistently deferred to agency determinations of their own investigative authority, and have generally refused to entertain challenges to agency authority in proceedings to enforce compulsory process." FTC v. Ken Roberts Co., 276 F.3d 583, 586 (D.C. Cir. 2001) (citing cases). Consistent with other courts of appeal, the Eleventh Circuit has held that "[t]he initial determination of the coverage question is left to the administrative agency seeking enforcement of the subpoena." Kloster Cruise, 939 F.2d at 922.

must be enforced."); EEOC v. Tire Kingdom, Inc., 80 F.3d 449, 450-51 (11th Cir. 1996); United States v. Fla. Azalea Specialists, 19 F.3d 620, 622-23 (11th Cir. 1994); Casey v. FTC, 578 F.2d 793, 799 (9th Cir. 1978) ("The district court's role in a subpoena enforcement proceeding is strictly limited where the subpoena is attacked for lack of agency jurisdiction. The subpoena must be enforced if the information sought is 'not plainly incompetent or irrelevant to any lawful purpose' of the FTC."). Thus, the Court's inquiry at the enforcement stage is limited. The Court addresses these questions in assessing whether to grant the FTC's request to enforce the CIDs.

1. Plausible argument that the FTC has jurisdiction to regulate data security and consumer privacy under Section 5

Section 5 does not specifically identify data security and consumer privacy as areas in which the FTC has jurisdiction to regulate. 15 U.S.C. § 45(n). Rather, courts interpret Section 5 as a statute that broadly confers authority on the FTC to investigate and regulate unfair practices that cause or are "likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." See 15 U.S.C. § 45(n); Genuine Parts Co. v. FTC, 445 F.2d 1382, 1391 (5th Cir. 1971) (FTC accorded "extreme breadth" in conducting investigations). The authority of the FTC under Section 5 to regulate unfair

practices is broadly construed by courts because it is impossible to define what constitutes unfair practices in a constantly changing and evolving economic climate. See FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 240, 244 (1972); Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1368 (11th Cir. 1988).

In determining the limits of the FTC's authority to investigate and address unfair practices regarding failures to employ reasonable data security measures, this Court is mindful that "[c]ourts have long held that consumers are injured for purposes of [Section 5 of the FTCA] not solely through the machinations of those with ill intentions, but also through the actions of those whose practices facilitate, or contribute to, ill intentioned schemes if the injury was a predictable consequence of those actions." FTC v. Neovi, 604 F.3d 1150, 1156-57 (9th Cir. 2010) (citing FTC v. Winsted Hosiery Co., 258 U.S. 483, 494 (1922) (holding that "[t]he honest manufacturer's business may suffer, not merely through a competitor's deceiving his direct customer, the retailer, but also through the competitor's putting into the hands of the retailer an unlawful instrument . . ."); FTC v. R.F. Keppel & Bro., Inc., 291 U.S. 304, 314 (1934) (holding candy retailer liable for unfair practices although manufacturer was responsible for the element of chance that made the practices unfair); Regina Corp. v. FTC, 322 F.2d 765, 768 (3d Cir. 1963) (explaining that "[w]ith respect to those instances where petitioner did not

contribute to the [misleading act], it is settled that [o]ne who places in the hands of another a means of consummating a fraud or competing unfairly in violation of the Federal Trade Commission Act is himself guilty of a violation of the Act") (quotation marks and citations omitted)).

"The statutory scheme at issue here 'necessarily gives the Commission an influential role in interpreting section 5 and in applying it to facts of particular cases arising out of unprecedented situations.'" Orkin Exterminating Co., 849 F.2d at 1367-68 (quoting FTC v. Colgate-Palmolive, Co., 380 U.S. 374, 385 (1965)). "Congress has not at any time withdrawn the broad discretionary authority originally granted the Commission in 1914 to define unfair practices on a flexible, incremental basis." Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 967 (D.C. Cir. 1985); see also Orkin, 849 F.2d at 1368 (FTC's Section 5 authority is a "broad mandate conferred upon the Commission by Congress."); FTC v. Windward Mktg., Inc., No. Civ.A. 1:96-CV-615F, 1997 WL 33642380, at *11 (N.D. Ga. Sept. 30, 1997) ("Congress has not enacted any more particularized definition of unfairness to limit the Commission's discretion.").

Although it is given broad discretion to determine what constitutes an unfair practice, the FTC's authority to investigate unfair practices using its subpoena enforcement power is not unlimited. Courts measure the validity of an FTC

subpoena against the purposes stated in the FTC resolution authorizing an investigation into specific practices. See 15 U.S.C. § 57b-1(i);[2] FTC v. Invention Submission Corp., 965 F.2d 1086, 1092 (D.C. Cir. 1992).

Respondents argue that the CIDs here are invalid because the 2008 Resolution was issued before the FTC learned of the existence of the 1,718 File and, in any event, is too vague to support the issuance of an administrative subpoena seeking information from LabMD. (See Ex. 2 to Pet. at 3). Respondents also assert that the FTC's claim of authority to regulate data security is not based on any threat of substantial injury to consumers, but only gross generalities.

As to Respondents' argument that the 2008 Resolution is vague and invalid, the Court disagrees. There is no dispute that the 2008 Resolution was validly issued by the Commission and the Court finds it sufficiently specifies the nature, scope, and subject matter upon which subpoenas and demands for information may

[2] The FTCA provides:

> Notwithstanding any other provision of law, the Commission shall have no authority to issue a subpoena or make a demand for information, under authority of this subchapter or any other provision of law, unless such subpoena or demand for information is signed by a Commissioner acting pursuant to a Commission resolution. The Commission shall not delegate the power conferred by this section to sign subpoenas or demands for information to any other person.

15 U.S.C. § 57b-1(i).

be made.[3] Respondent has not cited any legal authority, and the Court has found none, that invalidates an administrative agency's subpoena because it is issued based on authority in a resolution that pre-dates the identification of a specific issue of concern within the scope of that resolution. See Invention Submission Corp., 965 F.2d at 1092 (quoting FTC v. Carter, 636 F.2d 781, 789 (D.C. Cir. 1980)) ("clear that 'the validity of Commission subpoenas is to be measured against the purposes stated in the resolution, and not by reference to extraneous evidence'").

The Court also disagrees with Respondents' contention that there is no basis for the FTC to investigate and regulate data security and consumer privacy because there is no threat of substantial injury to consumers. The FTC presents sufficient information in its pleadings to support its claim that there is a significant and

[3] The 2008 Resolution states, under a heading entitled "Nature and Scope of Investigation," that it was adopted to permit the FTC:

> To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act [("FTCA")], 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

(Ex. 2 to Pet. at 3).

widespread impact and threat to consumers, including identity theft, that results from breaches of data security and consumer privacy. (See Pet'r's Supplemental Mem. in Supp. of Pet. to Enforce Civil Investigative Demand [20] at 9-10; Pet'r's Reply Mem. in Supp. of Pet. [15] at 8, 12-13). The Court finds that the FTC presents a plausible argument for the exercise of its jurisdiction to investigate and enforce in the realm of data security and consumer privacy—which it has done so in at least forty-four instances since 2000—in light of the threat of substantial consumer harm that occurs when consumers are victims of identity theft—a routine occurrence in the United States. See Pl.'s Rep. in Opp'n to Wyndham Hotels and Resorts' Mot. to Dismiss at 5, FTC v. Wyndham Worldwide Corp., Case No. 2:12-cv-01365-PHX-PGR (D. Ariz. filed June 26, 2012); Legal Resources, BCP Business Center, http://business.ftc.gov/legal-resources/29/35 (last visited Nov. 16, 2012) (citing enforcement actions); (Pet'r's Supplemental Mem. in Supp. of Pet. to Enforce Civil Investigative Demand at 9-10; Pet'r's Reply Mem. in Supp. of Pet. at 8, 12-13).

The Court also finds support for the conclusion that the FTC's argument is plausible regarding its jurisdiction because federal courts have recognized the FTC's authority under Section 5 to investigate and use its authority to address unfair practices regarding related data security and consumer privacy issues. See

FTC v. Pricewert, LLC, No. C-09-2407 RMW, 2010 WL 329913, at *2-*3 (N.D. Cal. 2010) (Section 5 used to address "distribution of illegal, malicious and harmful electronic content"); FTC v. CyberSpy Software, LLC, No. 6:08-cv-1872-Orl-31GJK, 2009 WL 455417, at *1 (M.D. Fla. Feb. 23, 2009) (Section 5 used to address marketing of a software program that could be used illegitimately to commit identity theft); FTC v. Accusearch, Inc., No. 06-CV-105-D, 2007 WL 4356786, at *1, *7-*8 (D. Wyo. Sept. 28, 2007), aff'd 570 F.3d 1187 (10th Cir. 2009) (Section 5 used to address the unauthorized disclosure of confidential customer phone records); FTC v. Seismic Entm't Prods., Inc., No. Civ. 04-377-JD, 2004 WL 2403124, at *2-*4 (D.N.H. 2004) (Section 5 used to address internet advertising methods that cause unauthorized changes to computers and that affect data security).

Although the Court finds there is significant merit to Respondents' argument that Section 5 does not justify an investigation into data security practices and consumer privacy issues, it is a plausible argument to assert that poor data security and consumer privacy practices facilitate and contribute to predictable and substantial harm to consumers in violation of Section 5 because it is disturbingly commonplace for people to wrongfully exploit poor data security and consumer privacy practices to wrongfully acquire and exploit personal consumer

information. Because the FTC's assertion of jurisdiction to issue its CIDs is premised on a plausible argument, the Court finds that Respondents' argument that the CIDs should not be enforced for a lack of jurisdiction is not a sufficient reason to deny the FTC's request for enforcement. See Kloster Cruise, 939 F.2d at 922.

2. Whether the information sought by the subpoena is unreasonable or "plainly incompetent or irrelevant to any lawful purpose [of the FTC]"

With regard to administrative subpoenas issued by the FTC, the Supreme Court has stated:

> Even if one were to regard [a] request for information . . . as caused by nothing more than official curiosity, nevertheless lawenforcing [sic] agencies have a legitimate right to satisfy themselves that corporate behavior is consistent with the law and the public interest.
>
> Of course a governmental investigation into corporate matters may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power. Federal Trade Comm. v. American Tobacco Co., supra. But it is sufficient if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant. 'The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable.' Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186, 208, 66 S.Ct. 494, 505, 90 L.Ed. 614, 166 A.L.R. 531.

See United States v. Morton Salt Co., 338 U.S. 632, 652-53 (1950).

Thus, "[t]he chief limitation on an investigation by an administrative agency is that it must meet the test of reasonableness." Genuine Parts Co., 445 F.2d at 1391 (citing Oklahoma Press Publishing Co. v. Walling, 327 U.S. at 208). The information sought by the FTC also must "not [be] plainly incompetent or irrelevant to any lawful purpose." See Kloster Cruise, 939 F.2d at 922 (quotations omitted). In seeking information in an investigation, the FTC is accorded "extreme breadth" by courts when evaluating its demands for testimony and documents. See Genuine Parts Co., 445 F.2d at 1391.

Furthermore, the burden of showing that an administrative subpoena is unreasonable is a heavy one because

> [s]ome burden on subpoenaed parties is to be expected and is necessary in furtherance of the agency's legitimate inquiry and the public interest. The burden of showing that the request is unreasonable is on the subpoenaed party. Further, that burden is not easily met where . . . the agency inquiry is pursuant to a lawful purpose and the requested documents are relevant to that purpose. Broadness alone is not sufficient justification to refuse enforcement of a subpoena. Thus courts have refused to modify investigative subpoenas unless compliance threatens to unduly disrupt or seriously hinder normal operations of a business.

See FTC v. Texaco, Inc., 555 F.2d 862, 882 (D.C. Cir. 1977).

The FTC here demands documents and testimony related to the public disclosure on P2P networks of Respondents' 1,718 File containing the names and

sensitive information of 9,000 consumers and LabMD's data security practices. The Court has reviewed the FTC's CIDs in this action and finds they are specific in scope, reasonably relevant to its investigation into LabMD's data security practices, and, even though LabMD has already produced a significant amount of material, are not duplicative or unreasonable. (See Ex. 2 to Pet. at 11-12; Ex. 3 to Pet. at 8). The Court finds that the demands in the CIDs—beyond being based on a plausible argument regarding the FTC's statutory authority and jurisdiction—are not too indefinite and the information sought is reasonably relevant to its investigation into Respondents' data security and customer privacy practices.

In light of the "sharply limited" "role of a district court in a proceeding to enforce an administrative subpoena," the Court finds the CIDs are required to be enforced because there is a plausible argument for the exercise of jurisdiction by the FTC and "the evidence sought is material and relevant to a lawful purpose of the agency." See Kloster Cruise, 939 F.2d at 922.

III. CONCLUSION

For the foregoing reasons,

IT IS HEREBY ORDERED that Petitioner's Petition [1] is **GRANTED**.

IT IS FURTHER ORDERED that, no later than December 15, 2012, Respondents shall comply with Petitioner's Civil Investigative Demands.

SO ORDERED this 26th day of November, 2012.

WILLIAM S. DUFFEY, JR.
UNITED STATES DISTRICT JUDGE

EXHIBIT
21

Document(1)

1. Atlanta medical lab facing off against FTC
   Client/matter: -None-

Atlanta medical lab facing off against FTC

Atlanta Business Chronicle

September 7, 2012 Friday

Length: 989 words

Byline: Amy Wenk

Body

A small *medical* company based in *Atlanta* is fighting a federal investigation into its data security practices - a potentially damaging blow to its reputation, says its founder.

The Federal Trade Commission (*FTC*) on Aug. 29 filed a petition in federal court to investigate LabMD Inc. and its CEO, Michael Daugherty, to determine whether the company had adequate data security for its *medical* records.

The federal agency says it obtained a copy of a 1,718-page spreadsheet that contained sensitive health information for about 9,000 of LabMD's patients, including Social Security numbers, birth dates and health insurance policy numbers, according to the petition.

"There is no allegation that anybody has done anything wrong," said Leslie Rice Melman, assistant general counsel for litigation for the *FTC*. She said the *FTC* is trying to investigate LabMD but the company has been unwilling to provide oral testimony and other documents.

"In most cases, in the end, we are able to get compliance without seeking the aid of the district court," Melman said. "Citizens have an obligation to respond and cooperate in a lawful government investigation."

Melman said a court hearing is set for Sept. 19 in the U.S. District Court for the Northern District of Georgia.

Daugherty contends his company is being unreasonably persecuted by the *FTC*. He said he's already spent about $500,000 fighting the investigation.

"We are guilty until proven innocent to these people," Daugherty said in a Sept. 5 interview with *Atlanta* Business Chronicle. "They are on a fishing expedition. We feel like they are beating up small business.

"There's no deception. There's not been a breach," he said.

Founded in 1996, LabMD performs *medical* testing services and specializes in tissue analysis for cancer. The company has about 35 employees and is headquartered at 2030 Powers Ferry Road.

Daugherty, a graduate of the University of Michigan, worked as a surgical sales rep before starting LabMD. He's served on the advisory board for the Private Bank of Buckhead for the past two years.

Matthew Smith

The trouble started for LabMD in May 2008 when, Daugherty said, he received a phone call from Pennsylania-based Tiversa Inc., saying the company had possession of a 1,718-page spreadsheet of health insurance billing information.

Tiversa specializes in providing security services for peer-to-peer networks, a component of the Internet that allows people to share digital content, such as music, movies and software. On its website, Tiversa says its technology can monitor more than 550 million users, issuing 1.8 billion searches a day.

Tiversa downloaded LabMD's spreadsheet in 2008 as part of a research project in collaboration with Dartmouth College, according to a 2009 report from the college. The research was backed with federal funds from the U.S. Department of Justice, the U.S. Department of Homeland Security and the National Science Foundation, among others.

Daugherty said Tiversa hounded LabMD to sign a service agreement to remedy any possible data security flaws in its network.

Daugherty said he refused to purchase any services from Tiversa during its several attempts to solicit business from LabMD via email in 2008.

In 2009, Daugherty said he was informed by his lawyer that Tiversa was going to hand over the downloaded spreadsheet to the federal government.

LabMD later sued Tiversa, accusing the company of stealing its property.

On Aug. 15, that lawsuit was dismissed due to a lack of personal jurisdiction, said Daugherty's general counsel, Stephen Fusco. LabMD currently is appealing that decision.

"This is a property theft case," Daugherty said. "[Tiversa] came in and affected our network."

The ***FTC*** began its investigation of LabMD in early 2010, requesting it send internal documents to be reviewed.

"We've always complied," Daugherty said. He said the company has six times submitted thousands of pages of documents to the ***FTC***. He also has visited Washington, D.C., twice to speak with the ***FTC***, he said. "We have nothing to hide."

According to Daugherty, when the ***FTC*** asked him to sign a consent decree, he refused. He said it would have required the business to undergo biannual audits for the next 20 years.

"That's where the road is lined with bombs," Daugherty said. "I won't let you assassinate my reputation."

In December 2011, the ***FTC*** issued formal demands to investigate LabMD.

The company subsequently filed a petition to reject the request to investigate, which was later overruled by the five-member commission appointed by the U.S. president that governs the ***FTC***.

One commission member dissented.

"Specifically, I am concerned that Tiversa is more than an ordinary witness, informant or 'whistle-blower,'" wrote Commissioner J. Thomas Rosch in a statement on June 21, 2012. "It is a commercial entity that has a financial interest in intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect

against similar infiltrations ... In my view, while there appears to be nothing per se unlawful about this evidence, the commission should avoid even the appearance of bias or impropriety by not relying on such evidence or information in this investigation."

The ***FTC*** says its staff cannot make a proper recommendation without testimony from Daugherty and LabMD.

"This is completely routine," the ***FTC***'s Melman said. "This is just how administrative agencies go about carrying out their mission of investigating whether there are unlawful practices."

Melman said it's unusual to have to file a petition in federal court to start an investigation. She said the last instance was about a year ago.

Daugherty said he won't give up his fight ***against*** the ***FTC***, no matter the costs.

"It's cheaper than our reputation."

Classification

Language: ENGLISH

Publication-Type: Newspaper

Subject: INVESTIGATIONS (93%); US FEDERAL GOVERNMENT (92%); LAW COURTS & TRIBUNALS (90%); CRIMINAL INVESTIGATIONS (90%); DATA SECURITY (90%); COMMERCE DEPARTMENTS (90%); INFORMATION SECURITY & PRIVACY (90%); WITNESSES (78%); ***MEDICAL*** RECORDS (78%); JUSTICE DEPARTMENTS (78%); HEALTH INSURANCE (78%); SPECIAL INVESTIGATIVE FORCES (78%); SMALL BUSINESS (78%); ***MEDICAL*** & DIAGNOSTIC LABORATORIES (78%); NATIONAL SECURITY (78%); RESEARCH & DEVELOPMENT (77%); PETITIONS (77%); US SOCIAL SECURITY (75%); SOCIAL SECURITY (75%); LAWYERS (73%); ***MEDICAL*** DIAGNOSTICS SCREENING & TESTING (73%); LAW ENFORCEMENT (73%); TESTIMONY (72%); INSURANCE POLICIES (70%); CORPORATE COUNSEL (69%); TEST LABORATORIES (68%); INTERNET & WWW (63%); COMPUTER NETWORKS (60%); COMPUTER SOFTWARE (60%)

Organization: FEDERAL TRADE COMMISSION (94%)

Geographic: ***ATLANTA***, GA, USA (92%); GEORGIA, USA (92%); MICHIGAN, USA (79%); UNITED STATES (94%)

Load-Date: September 7, 2012

EXHIBIT
22

FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy

Commission Alleges Exposure of Medical and Other Sensitive Information Over Peer-to-Peer Network

FOR RELEASE

August 29, 2013

TAGS: Health Care | Health Professional Services | Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security | Health

The Federal Trade Commission filed a complaint against medical testing laboratory LabMD, Inc. alleging that the company failed to reasonably protect the security of consumers' personal data, including medical information. The complaint alleges that in two separate incidents, LabMD collectively exposed the personal information of approximately 10,000 consumers.

The complaint alleges that LabMD billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network and then, in 2012, LabMD documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves.

The case is part of an ongoing effort by the Commission to ensure that companies take reasonable and appropriate measures to protect consumers' personal data.

LabMD conducts laboratory tests on samples that physicians obtain from consumers and then provide to the company for testing. The company, which is based in Atlanta, performs medical testing for consumers around the country. The Commission's complaint alleges that LabMD failed to take reasonable and appropriate measures to prevent unauthorized disclosure of sensitive consumer data – including health information – it held. Among other things, the complaint alleges that the company:

- did not implement or maintain a comprehensive data security program to protect this information;
- did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities to this information;
- did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;

did not adequately train employees on basic security practices; and

did not use readily available measures to prevent and detect unauthorized access to personal information.

The complaint alleges that a LabMD spreadsheet containing insurance billing information was found on a P2P network. The spreadsheet contained sensitive personal information for more than 9,000 consumers, including names, Social Security numbers, dates of birth, health insurance provider information, and standardized medical treatment codes. Misuse of such information can lead to identity theft and medical identity theft, and can also harm consumers by revealing private medical information.

P2P software is commonly used to share music, videos, and other materials with other users of compatible software. The software allows users to choose files to make available to others, but also creates a significant security risk that files with sensitive data will be inadvertently shared. Once a file has been made available on a P2P network and downloaded by another user, it can be shared by that user across the network even if the original source of the file is no longer connected.

“The unauthorized exposure of consumers’ personal data puts them at risk,” said Jessica Rich, Director of the FTC’s Bureau of Consumer Protection. “The FTC is committed to ensuring that firms who collect that data use reasonable and appropriate security measures to prevent it from falling into the hands of identity thieves and other unauthorized users.”

The complaint also alleges that in 2012 the Sacramento, California Police Department found LabMD documents in the possession of identity thieves. These documents contained personal information, including names, Social Security numbers, and in some instances, bank account information, of at least 500 consumers. The complaint alleges that a number of these Social Security numbers are being or have been used by more than one person with different names, which may be an indicator of identity theft.

The complaint includes a proposed order against LabMD that would prevent future violations of law by requiring the company to implement a comprehensive information security program, and have that program evaluated every two years by an independent, certified security professional for the next 20 years. The order would also require the company to provide notice to consumers whose information LabMD has reason to believe was or could have been accessible to unauthorized persons and to consumers’ health insurance companies.

The Commission vote to issue the administrative complaint and notice order was 4-0.

Because LabMD has, in the course of the Commission’s investigation, broadly asserted that documents provided to the Commission contain confidential business information, the Commission is not publicly releasing its complaint until the process for resolving any claims of confidentiality is completed and items in the complaint deemed confidential, if any, are redacted.

NOTE: The Commission issues an administrative complaint when it has “reason to believe” that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. The issuance of the administrative complaint marks the beginning of a proceeding in which the allegations will be tried in a formal hearing before an administrative law judge.

The Federal Trade Commission works for consumers to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop, and avoid them. To file a complaint in English or Spanish, visit the FTC’s online Complaint Assistant or call 1-877-FTC-HELP (1-877-382-4357). The FTC

enters complaints into Consumer Sentinel, a secure, online database available to more than 2,000 civil and criminal law enforcement agencies in the U.S. and abroad. The FTC's website provides free information on a variety of consumer topics. Like the FTC on Facebook, follow us on Twitter, and subscribe to press releases for the latest FTC news and resources.

CONTACT INFORMATION

MEDIA CONTACT:
Jay Mayfield
Office of Public Affairs
202-326-2181

STAFF CONTACT:
Robert Schoshinski
Bureau of Consumer Protection
202-326-3219

Related Cases

LabMD, Inc., In the Matter of

For Consumers

How To Keep Your Personal Information Secure

Identity Theft

Media Resources

Our Media Resources library provides one-stop collections of materials on numerous issues in which the FTC has been actively engaged. These pages are especially useful for members of the media.

Federal Trade Commission
BCP Business Center

FTC files data security complaint against LabMD

- By Lesley Fair
- August 29, 2013 - 11:32am

If your clients are focused on data security — and they should be — here's a development they'll want to know about. The FTC just filed an administrative complaint against Atlanta-based LabMD. The company does lab work for people across the country when their local doctors send in samples for testing. The primary allegation: that the company failed to reasonably protect the security of consumers' personal data, including medical information.

The lawsuit recounts two separate incidents. First, the FTC says a LabMD spreadsheet with insurance billing information was found on a peer-to-peer (P2P) file-sharing network. The spreadsheet had names, Social Security numbers, dates of birth, and health insurance info for more than 9000 people. What's more, the spreadsheet included standardized medical treatment codes.

P2P software is often used to share music, videos, and other stuff, but it comes with a substantial risk that sensitive documents can be inadvertently shared, too. And once a file is downloaded onto a P2P network, it's Katie, bar the door. It can be shared across the network even if the original source of the file isn't connected any more.

The FTC also alleges the Sacramento Police Department found LabMD documents in the possession of identity thieves. What was in the files? Names, Social Security numbers, and in some cases, bank account information for at least 500 people. According to the complaint, some of those SSNs are being used (or have been used) by more than one person with different names. That could be a possible indicator of ID theft.

Among other things, the complaint alleges that LabMD:

- Didn't implement or maintain a comprehensive data security program to protect sensitive information;
- Didn't use readily available measures to identify commonly known or reasonably foreseeable risks and vulnerabilities;

- Didn't use adequate measures to prevent LabMD employees from accessing information not needed to perform their jobs;
- Didn't train their people on basic security practices; and
- Didn't use readily available measures to prevent and detect unauthorized access to personal data.

At this point, we'd usually suggest you read the complaint for details, but we can't right now. In the course of the investigation, LabMD has broadly asserted that documents provided to the FTC contain confidential business information. So the complaint won't be publicly available until those matters are resolved.

The case is pending before an Administrative Law Judge.

0 Comments | Commenting Policy

News from the Federal Trade Commission - September 2013

Federal Trade Commission sent this bulletin at 09/17/2013 09:35 AM EDT

Candid Camera

The FTC has settled its charges against TRENDnet, a company that markets video cameras for remote home monitoring. According to the FTC, TRENDnet marketed its SecurView cameras as secure for home security and baby monitoring, but the cameras had faulty software that left them open to online viewing. A hacker exploited this flaw, and eventually others posted links to the live feeds of nearly 700 cameras that displayed babies asleep in their cribs, young children playing, and adults going about their daily lives. This is the agency's first action against a marketer of an everyday product with online interconnectivity – commonly referred to as the "Internet of Things."

Jesta Minute

Global mobile marketer Jesta Digital, LLC, must provide refunds to consumers and pay an additional $1.2 million to settle FTC charges that they "crammed" unwanted charges onto people's cell phone bills. According to the Commission's complaint, Jesta –which also does business as Jamster – ran phony virus-scan ads on Android mobile devices while people played the Angry Birds app. Jesta charged

as companies develop more devices that connect to the Internet."

— FTC Chairwoman Edith Ramirez

CAR-dinal Rule

Two car dealers have agreed to settle the FTC's charges that they falsely advertised certain discounts for their vehicles. According to the FTC, Timonium Chrysler, Inc., and Ganley Ford West, Inc., advertised discounts and prices that were not available to the typical driver.

Affordable Care Act

The FTC will host a roundtable September 19to discuss how to empower and protect people from scammers when healthcare marketplaces open in October under the Affordable Care Act (ACA). The roundtable will take place at the FTC's Conference Center in Washington, DC. The event will be webcast. To register to attend, email your name and organization to tthomas@ftc.gov.

Protecting Personal Medical Data

The FTC filed a complaintagainst LabMD, Inc., a medical testing laboratory, alleging that the company failed to reasonably protect the security of consumers' personal data and medical information. The complaint alleges that LabMD billing information for more than 9,000 people was found on a peer-to-peer (P2P) file-sharing network. Subsequently, LabMD documents containing the sensitive personal information of at least 500 people were found in the hands of identity thieves.

IN OTHER NEWS:

- FTC Signs Memorandum of Understanding with Nigerian Consumer Protection and Criminal Enforcement Authorities
- FTC Returns Additional $950,000 to Consumer Victims in DVD Vending Scam
- Precious Metal Marketers Agree to Settle FTC Charges
- FTC Seeks Public Comment on Imperium, LLC, Proposal for Parental Verification Method Under COPPA Rule

More >

SHARE THIS:

- Phone cramming – surely you Jesta. **http://go.usa.gov/DkrY**
- Keeping the check checkers in check. **http://go.usa.gov/DkrB**
- Use IP cameras safely. **http://go.usa.gov/DkrQ**
- Listen up – an audio tip about online payday loans! **http://go.usa.gov/Dkrw**

EXHIBIT

23

FTC Says Authority Extends To LabMD's Health Data

By **Allison Grande** 0 Comments Share us on:

Law360, New York (November 27, 2013, 6:30 PM ET) -- The Federal Trade Commission fired back Wednesday at LabMD Inc.'s contention that federal health privacy law trumps the agency's data security claims, arguing that it has a broad mandate to protect personal information that complements health regulators' similar authority.

The FTC's response — which is dated Nov. 22 but was posted on the docket in the administrative action Wednesday — pushes back at the **medical testing laboratory's contention** that the agency cannot maintain its allegations that the company failed to implement reasonable data security protections because Congress has already given the U.S. Department of Health and Human Services' Office for Civil Rights the sole authority to set and enforce rules for securing confidential patient medical information.

In its reply, the commission counters that neither the Health Insurance Portability and Accountability Act nor the Health Information Technology for Economic and Clinical Health Act provides HHS with the exclusive authority over the security of consumers' sensitive personal information. Rather, the statutory framework provides the FTC and HHS with "concurrent and complementary jurisdiction" to protect consumers' sensitive health information, the agency contends.

"Congress charged HHS with improving 'the efficiency and effectiveness of the health care system by, among other things, establishing standards with respect to the privacy of individually identifiable health information,'" the commission wrote. "The FTC has a broader but complementary mandate to prevent deceptive or unfair practices, including the failure to provide reasonable and appropriate security for personal information."

The two agencies also have complementary remedies, with the FTC able to seek equitable monetary and injunctive relief under Section 5 of the FTC Act and the HHS given the authority to seek civil penalties under HIPAA and HITECH, and have exercised their prosecutorial discretion in the past to bring both separate and coordinated actions that involve the failure to protect sensitive personal health information, according to the commission.

In its motion, the FTC specifically cites a pair of investigations and settlements reached with Rite Aid Corp. in 2010 and CVS Caremark Corp. in 2009. Both enforcement actions included claims advanced by the regulators under their respective authorities that the pharmacies had failed to protect their customers' health information.

The motion also rejects LabMD's suggestion that specific statutes like HIPAA necessarily repeal general ones like the FTC Act, saying the argument is grounded in a misinterpretation of a canon of statutory construction and that no sector-specific data security statute abrogates the FTC's data security jurisdiction under the FTC Act.

"HIPAA does not conflict, irreconcilably or otherwise, with the consumer protection mandate of the FTC Act, and therefore both statutes should be regarded as effective," the FTC contends. "The application of Section 5 of the FTC Act does not render HIPAA and the HITECH Act superfluous."

Because HIPAA and HITECH were enacted well after the FTC was given the authority to protect consumers from unfair and deceptive practices under Section 5, any intention by

Congress to preempt or repeal the FTC's ability to protect consumers' information by using its unfairness authority would have needed to be "clear and manifest," an element missing from both health privacy statutes, the regulator claims.

The ability of the FTC to force companies to maintain certain data security standards under its authority to protect consumers from practices that are likely to cause substantial injury is at the heart of the instant action, as well as a **similar fight being mounted** by Wyndham Worldwide Corp. in the District of New Jersey.

The pair of cases, which are the first to challenge the regulator's data security authority, both allege the FTC lacks jurisdiction to regulate how a business protects consumer information.

Besides responding to LabMD's novel HIPAA-related claim, which the hotel chain cannot raise, the FTC in its Nov. 22 response also shot back at the common accusation that Congress had never expressly granted authority to the FTC to declare that companies must engage in "reasonable" practices to prevent unauthorized access to personal information.

The FTC countered that its action against LabMD "falls squarely within" the "broad" authority it has under Section 5 to protect consumers against unfair business practices, and that the fact that Congress has given the agency additional tools to pursue data security through the enactment of statutes such as the Children's Online Privacy Protection Act and the Gramm-Leach-Bliley Act does not negate its unfairness authority.

"The complaint pleads specific facts, which, if proven, establish that LabMD is liable for committing an unfair practice under Section 5," the commission wrote. "The … consideration of respondent's motion to dismiss should thus end here."

LabMD is represented by Reed Rubinstein of Dinsmore & Shohl LLP and Michael D. Pepson of Cause of Action.

The case is In the Matter of LabMD Inc., docket number 9357, before the Federal Trade Commission.

--Editing by Philip Shea.

Related Articles

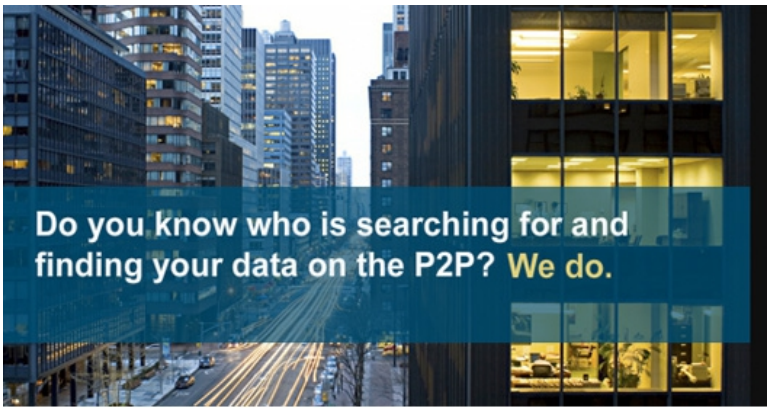
LabMD Unleashes Trump Card In FTC Data Security Fight
FTC Sues To Get Patient Data Spreadsheet From LabMD
LabMD Slams 'Oppressive' FTC Subpoenas In Data Breach Row
FTC's Increasingly Aggressive Assertion Of Authority
LabMD Didn't Do Enough To Protect Customer Data, FTC Says

Medical lab allegedly exposed customer info on P2P, claims it was the victim

Billing info was exposed on a P2P network because of poor security, FTC says.

by **Jon Brodkin** - Aug 29, 2013 7:40 pm UTC

IDENTITY 38



Security company Tiversa uncovered confidential health care information by scanning P2P networks.

Tiversa

A medical testing laboratory called LabMD has been accused of exposing the personal information of about 10,000 customers on a peer-to-peer file sharing network.

The company has been fighting the claims, saying a security firm that uncovered the breach victimized LabMD by downloading a large spreadsheet containing sensitive customer information.

The US Federal Trade Commission today said it filed a complaint which "alleges that LabMD billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network and then, in 2012, LabMD documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves."

The lab is based in Atlanta but performs medical tests for consumers nationwide.

Police in Sacramento, CA, found in 2012 that identity thieves had possession of LabMD documents containing names, Social Security numbers, and bank account information for at least 500 people. "[A] number of these Social Security numbers are being or have been used by more than one person with different names, which may be an indicator of identity theft," the FTC said. The complaint also alleges that "a LabMD spreadsheet containing insurance billing information was found on a P2P network," the FTC said. "The spreadsheet contained sensitive personal information for more than 9,000 consumers, including names, Social Security numbers, dates of birth, health insurance provider information, and standardized medical treatment codes."

LabMD allegedly failed to take proper precautions when handling sensitive data. The FTC said LabMD "did not implement or maintain a comprehensive data security program to protect this information; did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities to this information; did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs; did not adequately train employees on basic security practices; and did not use readily available measures to prevent and detect unauthorized access to personal information."

Although identity thieves got hold of financial details for more than 500 people, LabMD's troubles go

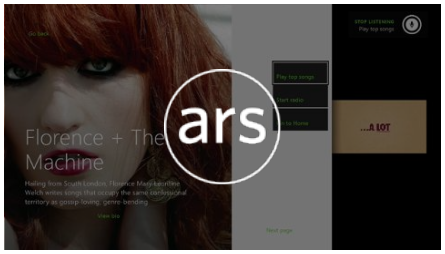
TOP FEATURE STORY

FEATURE STORY (3 PAGES)

The State of Smartphones in 2013, Part II: Would you like to play a game?

You picked your platform and your phone, now pick out some games and play!

WATCH ARS VIDEO



Xbox One Voice Command Test

A quick stress test shows just how much you can do with Xbox One voice commands

STAY IN THE KNOW WITH

LATEST NEWS

JUST A FLESH WOUND

BlackBerry tells customers that it's not dead—yet

UP AND AWAY

India, China send probes out of this world

Aging cells share features with cancer

CHEATERS PREFER WALLCLOCKS

College says time's up for cheaters,

Although identity thieves got hold of financial details for more than 500 people, LabMD's troubles go back to an earlier incident in May 2008, when a security company called Tiversa for peer-to-peer networks came across the 1,718-page spreadsheet of health insurance billing information, according to a story last year by the *Atlanta Business Chronicle*.

The newspaper paraphrased an FTC official as saying the commission was "trying to investigate LabMD but the company has been unwilling to provide oral testimony and other documents." LabMD CEO Michael Daugherty claimed the FTC is "on a fishing expedition" and "beating up small business."

The FTC denied a petition by LabMD to quash the civil investigative demands made by the agency. LabMD had claimed it's the victim in this case, saying the spreadsheet "was illegally downloaded from LabMD's computers in 2008." The spreadsheet is referred to as the "1,718 File" in legal documents.

LabMD filed suit against Tiversa, alleging violations of the US Computer Fraud and Abuse Act and the Georgia Computer Systems Protection Act. LabMD said the security firm refused to destroy its copies of the spreadsheet and tried to get LabMD to "purchase its security services in order to 'remediate' any issues" involving the spreadsheet. "Tiversa ... was and is running an extortionist scheme whereby it uses its government-funded technology to penetrate computer networks, download confidential files, and then sell the files back to the owners under the guise of providing network security," LabMD claimed in its petition to the FTC.

Tiversa had teamed up with Dartmouth College to search peer-to-peer networks for files related to health care firms. It appears to have been standard white hat hacking for the purposes of identifying security problems before criminals do.

LabMD's lawsuit was thrown out because of a lack of jurisdiction, due to Tiversa not conducting business in Georgia. According to a US District Court ruling, the spreadsheet "was created and stored on a LabMD computer. ... Defendants accessed LabMD's computers and networks, which must have been connected to the peer-to-peer network, and downloaded the 1,718 File."

In its unsuccessful petition to the FTC, LabMD said that Tiversa testified before Congress in 2009 that it "deployed newly developed P2P search technology that allowed it to penetrate even 'the most technologically advanced' computer despite the presence of 'firewalls and encryption.' It was with this technology ... that Tiversa and Dartmouth downloaded the 1,718 File."

Although the FTC described the complaint in a press release today, it did not release the document in full. "Because LabMD has, in the course of the Commission's investigation, broadly asserted that documents provided to the Commission contain confidential business information, the Commission is not publicly releasing its complaint until the process for resolving any claims of confidentiality is completed and items in the complaint deemed confidential, if any, are redacted," the FTC said.

LabMD, which describes itself as a "cancer detection facility that specializes in analysis and diagnosis of blood, urine, and tissue specimens for cancers, micro-organisms and tumor markers," did not take kindly to the FTC's latest action.

"The Federal Trade Commission's enforcement action against LabMD based, in part, on the alleged actions of Internet trolls, is yet another example of the FTC's pattern of abusing its authority to engage in an ongoing witch hunt against private businesses," LabMD said in a statement sent to Ars. "The allegations in the FTC's complaint are just that: allegations. LabMD looks forward to vigorously fighting against the FTC's overreach by seeking recourse through the available legal processes. The FTC has repeatedly overstepped its statutory authority under Section 5 of the Federal Trade Commission Act and the FTC does not have the authority to bring this enforcement action."

The FTC's proposed remedy is for LabMD to implement a "comprehensive information security plan" and provide notice to consumers whose information was leaked.

The administrative complaint just issued by the FTC "marks the beginning of a proceeding in which the allegations will be tried in a formal hearing before an administrative law judge," the commission said.

bans all watch-wearing during exams

VENI, VIDI, EMITI

Cyber Monday Dealmaster: Buy stuff in the comfort of your own home

HOW MUCH TO TIP A DRONE?

Amazon unveils "Prime Air," a plan to deliver by drone in just 30 minutes

Indeed. It shows a fundamental misunderstanding of P2P. They seem to think that the file was inaccessible until the researchers broke in and grabbed it using "P2P technology", which is roughly akin to saying that your bank vault was impenetrable until a police officer walked in through one of the missing walls and told you you had a problem.

So, 2008, any guesses as to what the P2P program was that they apparently set to share the entire HDD? Was Limewire still popular then?

Edit: Actually, a better analogy would be a police officer walking up to a bank that had a sign on its vault (which was sans door) saying "Take what you want! Everything must go!", pointing out the problem to management, and then being taken to court for theft.

193 posts | registered Feb 12, 2008

---

snowman<ca> | Ars Praetorian jump to post

I am going out on a limb and guessing their IT department was understafed and there arguments were made by people who do not understand either what was done wrong, what they should be doing or what was needed to fix the problem.

490 posts | registered Sep 2, 2008

READER COMMENTS 38

Jon Brodkin / Jon is Ars Technica's senior IT reporter, covering business technology and the impact of consumer tech on IT. He also w rites about tech policy, the FCC and broadband, open source, virtualization, supercomputing, data centers, and w ireless technology.
@JBrodkin

← OLDER STORY | NEWER STORY →

YOU MAY ALSO LIKE

HEALTHWATCH
THE HILL'S HEALTHCARE BLOG

August 29, 2013, 04:42 pm

FTC: Medical lab exposed 10K patients to identity fraud

By Elise Viebeck

Thursday's complaint highlights efforts to fight health-related identity fraud as information technology makes records more vulnerable to theft.

The complaint was administrative, meaning the allegations will eventually be tried before an administrative judge.

"The unauthorized exposure of consumers' personal data puts them at risk," said Jessica Rich, Director of the FTC's Consumer Protection Bureau, in a statement.

"The FTC is committed to ensuring that firms who collect that data use reasonable and appropriate security measures."

LabMD released a statement saying the FTC lacks the authority to file its complaint and accusing the agency of a conducting a "witch hunt" against business.

"The Federal Trade Commission's enforcement action against LabMD based, in part, on the alleged actions of Internet trolls, is yet another example of the FTC's pattern of abusing its authority," the company stated.

"LabMD looks forward to vigorously fighting against the FTC's overreach by seeking recourse through the available legal processes."

—This post was updated Thursday at 3:44 p.m. with LabMD's statement.

MORE OTHER HEADLINES

Poll: Public happier with own healthcare than nation's

Obama nominates new surgeon general

House votes to extend research into premature births, study HIV organ donations

More Other Headlines
Other News RSS feed

MOST POPULAR | EMAILED | DISCUSSED

More Videos »

MORE FROM THE WEB

FTC FILES SUIT AGAINST MEDICAL LABORATORY: A ROADMAP TO AVOID FAILING TO PROTECT CONSUMER PRIVACY

By Paul C. Van Slyke and Tammy Woffenden

Paul C. Van Slyke, a partner in the Houston office of Locke Lord LLP, advises clients in the areas of intellectual property, advertising, promotions, media, technology, anti-counterfeiting, privacy, data security, and publishing law. He teaches Advertising & Marketing Law at the University of Houston Law School.

Tammy Ward Woffenden, an associate in the Austin, Tex., office of Locke Lord LLP, focuses on transactional, regulatory, and administrative health law issues. Her areas of experience include HIPAA privacy compliance, review of contractual arrangements involving health care providers, health care provider licensure and certification matters, and mergers of health care entities.

The Federal Trade Commission filed an administrative complaint (link is to redacted form of the complaint), Docket No. 9357, recently against a medical testing laboratory, LabMD, Inc., alleging that the company failed to reasonably protect the security of consumers' personal information, and that such failures subjected consumers' personal information (in some instances including names, Social Security numbers, dates of birth, and healthcare-related information) to two separate security incidents. In the first incident, a spreadsheet was found online on a peer-to-peer ("P2P") network. In the second incident, the Sacramento Police Department found LabMD documents containing sensitive personal information of at least 500 consumers in the hands of identity thieves. Although some of the information involved was healthcare related, there are lessons to be learned by companies that handle personal information in any industry.

BACKGROUND

In a press release, the FTC said this case is part of an ongoing effort by the Commission to ensure that companies take reasonable and appropriate measures to protect consumers' personal data. "The unauthorized exposure of consumers' personal data puts them at risk," said Jessica Rich, Director of the FTC's Bureau of Consumer Protection. "The FTC is committed to ensuring that firms who collect that data use reasonable and appropriate security measures to prevent it from falling into the hands of identity thieves and other unauthorized users."

The FTC Complaint alleges that LabMD failed to take reasonable and appropriate measures to prevent unauthorized disclosure of sensitive consumer information — including health information — it collected and stored. Among other things, the Complaint alleges that the company:

• Did not implement or maintain a comprehensive security program to protect the sensitive consumer information;

• Did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities to that information;

• Did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;

• Did not adequately train employees on basic information security practices; and

• Did not use readily available measures to prevent and detect unauthorized access to personal information.

SECURITY RISK OF PEER-TO-PEER NETWORK SOFTWARE

As noted above, the complaint alleges that a testing laboratory spreadsheet containing insurance billing information was found on a P2P network. P2P network architecture is commonly used to share music, videos, and other materials with other users of compatible software, and may create significant security risks that files with sensitive information will be inadvertently shared. It is well known that P2P software used in a company network creates significant security risks. Once a file containing personal information has been made available on a P2P network and downloaded by another, it can be shared by that user across the network even if the original source of the file is no longer connected.

PROPOSED ORDER HAS ONEROUS REQUIREMENTS.

Like most FTC complaints dealing with consumer information, the FTC complaint contains a proposed agreed order that would prevent future violations of law, but also contained some unpleasant and onerous requirements, including:

• To implement a comprehensive written information security program;

• To require that the security program be evaluated every two years by an independent, certified security professional for the next twenty years; and

• To require the company to provide notice to consumers whose information the testing laboratory has reason to believe was, or could have been, accessible to unauthorized persons and to consumers' health insurance companies as well.

FTC COMPLAINT IS FOUNDED ON ITS UNFAIRNESS AUTHORITY

The FTC complaint bases its jurisdictional authority under the unfairness clause of Section 5 of the FTC Act, rather than its deceptiveness authority; *i.e.*, "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful" under Section 5 of the FTC Act. Since 1980 when the FTC adopted the Unfairness Policy Statement, many privacy actions brought by the FTC have been founded on its deceptiveness authority. During this period complaints were largely based on a representation to the public of a certain standard of privacy and a failure to live up to that standard as an act of deceptiveness. The Unfairness Policy Statement articulates a three-part test to determine whether the consumer injury is sufficient to make the practice unfair. The injury

1. must be substantial;

2. must not be outweighed by countervailing benefits to consumers or competition that the practice produces; and

3. must be an injury that consumers themselves could not reasonably have avoided.

The FTC filed this case under its unfairness authority of Section 5 of the FTC Act. The complaint alleges the three elements required by the Unfairness Policy Statement, namely:

1. "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."

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

3. "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."

FTC COMPLAINT DOES NOT COVER ADDED HIPAA OBLIGATIONS AND PENALTIES

Although the FTC complaint does not address potential violations of the Health Insurance Portability and Accountability Act ("HIPAA"), health care providers qualifying as "covered entities" under HIPAA are required to safeguard Protected Health Information ("PHI") and Electronic PHI in a manner that prevents unauthorized use or disclosure. Failure to do so may be a violation of HIPAA and is potentially subject to significant civil penalties.

Since 2009, covered entities that experience a breach of unsecured PHI are required to report the incident to the U.S. Department of Health and Human Services, Office of Civil Rights ("OCR"), contact affected individuals and, depending on the size of the breach, notify local media. OCR has been particularly active with enforcement measures relating to breaches of unsecured PHI caused by lack of adequate security measures, including failure to encrypt data, wipe equipment such as photocopies and laptops that store protected information, and use adequate technical safeguards to protect data that becomes available online. Covered entities, and their contractors who use and access PHI on the covered entity's behalf, are required to conduct ongoing security risk assessments to identify and resolve such system vulnerabilities.

FTC ISSUES CIVIL INVESTIGATIVE DEMANDS TO LABMD

The FTC has served Civil Investigative Demands ("CIDs") with a subpoena for documents and interrogatories seeking information on LabMD and its President Michael J. Daugherty. They responded by filing two petitions to limit or quash the CIDs before the FTC. On April 20, 2012, the FTC responded in a letter denying the two petitions in a ruling by FTC Commissioner Julie Brill acting as a delegate on behalf of the Commission. Among other grounds, the FTC ruled that the complaint is not required to allege under Section 5 that actual harm has occurred to consumers, but must allege, and did allege, only that "a failure to implement reasonable security measures may be an unfair act or practice if the failure is likely to cause harm. No showing of actual harm is needed."

FTC Commissioner J. Thomas Rosch issued a dissenting statement concurring with the decision to enforce the document subpoena. Commissioner Rosch, however, criticized Commissioner Brill's ruling on the petitions for failing to limit the scope of the CIDs to require production of a spreadsheet containing sensitive personally identifiable information regarding approximately 9,000 patients that was originally discovered through the efforts of Dartmouth Professor M. Eric Johnson and Tiversa, Inc.

In its answer to the compliant, LabMD adamantly denies the allegations of the complaint and takes the position that §5 does not give the FTC authority to regulate the acts and practices the FTC complained about. The answer states that the FTC's actions are arbitrary, capricious and an abuse of discretion. It also alleges that the FTC has not published any guidelines that clarify the types of data security practices it has the ability and authority to enforce and regulate in order to give fair notice.

The FTC has appointed Chief Administrative Law Judge D. Michael Chappell to take testimony and receive evidence at a hearing scheduled for April 28, 2014.

TAKEAWAYS

This case is a reminder that the FTC will take action if it believes a company has failed to provide adequate security measures to protect sensitive personal information. Other lessons to take away from this case are:

• Under its consumer protection jurisdiction, the FTC may extend the finding of failures to protect personal information to be an "unfair" practice under the FTC Act.

• Many companies are under FTC scrutiny if they collect, store or distribute consumer personal information such as names linked to Social Security numbers, dates of birth, and credit card account numbers, regardless of whether the company is primarily in the consumer goods business. That would include, for example, retailers, certain lenders, and, as in this case, a healthcare provider.

• The FTC will carefully scrutinize companies not only for having what constitutes appropriate security programs, but also what are the effectiveness of those security programs.

• Companies should be aware of the risks posed by P2P network sharing protocols.

• The FTC may look at the existence and depth of employee training regarding consumer security information, as well as measures to detect incidents of unauthorized access.

• The orders typically sought by the FTC in these matters include onerous requirements that require companies to take affirmative, and potentially intrusive, actions for years, or even decades.

The Big Story

FTC: Medical lab's lax security led to data leak

By **ANNE FLAHERTY**
— Aug. 29, 2013 3:46 PM EDT
Home » **Federal Trade Commission** » FTC: Medical lab's lax security led to data leak

WASHINGTON (AP) — The Federal Trade Commission on Thursday accused a small Atlanta-based medical lab that specializes in cancer detection of not doing enough to protect its patients' online records, resulting in the leak of Social Security numbers and birth dates of more than 9,000 consumers.

The complaint against LabMD describes what many consumers fear: being forced to hand over personal information to a doctor's office or hospital, not knowing how that data is handled or who has access to it, only to become vulnerable to identity theft. The allegations also raise questions about the federal government's push for the health care industry to swap paper for electronic records to save money when doing so relies on cybersecurity investments by private companies.

In a statement, LabMD said the company "looks forward to vigorously fighting against the FTC's overreach by seeking recourse through the available legal processes."

Jessica Rich, director of the FTC's bureau of consumer protection, said LabMD's practices put consumers at serious risk of identity theft.

"The FTC is committed to ensuring that firms who collect that data use reasonable and appropriate security measures to prevent it from falling into the hands of identity thieves and other unauthorized users," she said in a statement.

More than half of doctors' offices and 4 out of 5 hospitals have transitioned from paper to electronic medical records, according to the government. Moving to computerized records is the rare consensus issue in health care, enjoying support from across the political spectrum. Taxpayers have already contributed more than $14 billion to help speed the move through an incentive program that was part of the Obama administration's economic stimulus package.

The hope was that going digital would make caring for patients safer and less costly by helping avoid medical mistakes and cutting down on duplicative tests. But concerns have also surfaced about patient privacy and vulnerability to fraud. And progress has been mixed in getting medical computers from different offices to talk to each other, the key to a seamlessly efficient system.

A pair of reports in 2011 by the Health and Human Services inspector general warned that the drive to connect hospitals and doctors electronically was being layered on top of a system that already has privacy problems. The administration said in response it would pursue stronger safeguards.

The complaint filed Thursday means that the allegations will be tried in a formal hearing before an administrative law judge. The FTC wants the judge to order LabMD to institute a comprehensive information security program with