Exhibit A

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

LabMD, INC.	)	
	)	
Plaintiff,	)	CIVIL ACTION FILE
	)	NO. 1:14-CV-810-WSD
v.	)	
	)	ATLANTA, GEORGIA
FEDERAL TRADE COMMISSION	)	
	)	
Defendant.	)	
	)	

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

Wednesday, May 7, 2014

APPEARANCES OF COUNSEL:

For the Plaintiff: KILPATRICK TOWNSEND & STOCKTON LLP
(By: Ronald L. Raider
William D. Meyer)
Burleigh Lavisky Singleton)

DINSMORE & SHOHL LLP
(By: Reed D. Rubinstein)

For the Defendant: U.S. DEPARTMENT OF JUSTICE
(By: Lauren Fascett
Perham Gorji
Joel Marcus)

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

I N D E X

Witness	*Page*
MICHAEL JOHN DAUGHERTY	
Direct (By Mr. Raider)	5
Cross (By Mr. Gorji)	32
Redirect (By Mr. Raider)	57
CLIFF BAKER	
Direct (By Mr. Meyer)	58

Wednesday Morning Session

May 7, 2014

9:44 a.m.

-- -- --

P R O C E E D I N G S

-- -- --

(In open court:)

THE COURT: Good morning, everybody.

This is the hearing that is scheduled pursuant to my amended scheduling order which is dated April 9th this year. It's a hearing on the motion for preliminary injunction that's been requested by LabMD.

And absent anything that you want to discuss before we start, I would say let just get started. Any objection to doing that?

MR. RAIDER: No, Your Honor.

MS. FASCETT: No, Your Honor.

THE COURT: All right. And, LabMD, this is your hearing. You may begin.

MR. RAIDER: Thank you, Your Honor.

We would like to start by presenting some live testimony from Mr. Daugherty.

THE COURT: That would be fine.

MR. RAIDER: We also have Mr. Baker here.

Is it okay that he sits in the back or do you want

him out in the witness room?

THE COURT: Do you want him sequestered?

MS. FASCETT: I don't think that's necessary, Your Honor.

THE COURT: I agree.

Okay. Let's begin, then.

(The oath is given by the Courtroom Deputy Clerk.)

MR. RAIDER: Your Honor, just as Mr. Daugherty is getting some water, we have presented a notebook with all of the exhibits that plaintiff has on its exhibit list, and we will be using some of those in his examination.

So the witness has a copy, government counsel has a copy, and I think a copy has been made available to you.

THE COURT: I have got it.

And let's make sure all the appearances are noted on the record.

I guess we have Mr. Rubinstein, Mr. Singleton, Mr. Meyer, Mr. Raider for LabMD; is that correct?

MR. RAIDER: Yes.

THE COURT: And for the FTC, Ms. Fascett, Mr. Gorji is it?

MR. GORJI: Correct, Your Honor.

THE COURT: And Mr. Marcus, who I don't think has made an appearance in the case.

MR. MARCUS: That's correct. For the FTC, I am

just serving as of counsel here. I would be happy to enter an appearance if you would like.

THE COURT: Well, I mean, if you are just sitting there because you are an observer and not in the case, that's fine. But if you are in the case, you need to make an appearance.

MR. MARCUS: I will do that, Your Honor.

THE COURT: And please do that today.

All right. Let's begin.

MR. RAIDER: And, Your Honor, just to introduce myself as counsel for LabMD, I am Mr. Raider.

THE COURT: All right.

-- -- --

MICHAEL JOHN DAUGHERTY

being first duly sworn by the Courtroom Deputy Clerk, testifies and says as follows:

-- -- --

DIRECT EXAMINATION

BY MR. RAIDER:

Q. Would you please state your name for the record?

A. Michael John Daugherty.

Q. What is your role at plaintiff LabMD?

A. I'm the founder and CEO of LabMD.

Q. How long have you been CEO of LabMD?

A. Since 1996.

Q. What services has LabMD offered?
A. We are a medical laboratory doing cancer detection, tumor markers, bacterial detection in the urology marketspace.
Q. What services are you currently offering?
A. Currently we are billing services for prior specimens that were tested and access to medical records for the physicians and -- physicians that need to still have access.
Q. And when did you stop offering cancer detection testing services?
A. Our last specimen I believe was taken around the 9th of January of 2014 and our last result was released around January 15th, 2014.
Q. And what caused LabMD to stop offering cancer detection services?
A. The overriding cloud and draining ongoing investigation by the Federal Trade Commission.
Q. Could you turn to Tab 14 in your notebook?
A. Okay, I am in front of 14.
Q. And what is Exhibit 14?
A. 14 is the letter that I sent out to physicians, administrators, nurses and support staff of our client base on the 6th of January, 2014, letting them know we would no longer be accepting specimens so that they could make arrangements for other -- for their patients for future

medical testing.

Q. And if you would look at the third paragraph, could you please explain the reasons you provided to your clients for your business reason?

A. I said that FTC has subjected LabMD to years of debilitating investigation and litigation regarding an alleged patient information data security vulnerability without standards, information or congressional approval and without a consumer victim from the alleged breach, which is in quotations.

The FTC has taken upon itself to spend your tax dollars to ruin LabMD and regulate medical data security over and above HIPAA.

THE COURT: And do you intend to introduce this?

MR. RAIDER: Yes.

THE COURT: Well, before you publish it, don't you think you should do that?

MR. RAIDER: We were going to offer to tender the exhibits at the end unless there was an objection made to the exhibit.

THE COURT: Well, have you worked that out with the FTC?

MR. RAIDER: We have not.

THE COURT: All right. Well, you probably shouldn't publish anything until it's been introduced in

evidence, and basically that's what Mr. Daugherty has done. So you can either see if there is an objection, and if there is --

MS. FASCETT: There is no objection, Your Honor.

THE COURT: Then it's admitted. But you need to do that for each of the exhibits.

MR. RAIDER: Okay. Thank you, Your Honor. We will.

BY MR. RAIDER:

Q. Where are LabMD's records today?

A. LabMD's records are in the cooperate condominium and the basement of my residence.

Q. What outside sources have access to your servers in the condo?

A. There is a support volunteer that's helping who has had years of experience in medical urology office space. He's helping with the billing and winding down and answering questions. And then myself.

Q. Is there remote access to the servers?

A. There is no remote access except to the billing software. There is no remote access to any of the vast majority of electronic records in the laboratory information system.

Q. The FTC has issued a proposed order addressing LabMD's future conduct. What are the obligations the FTC has

proposed to be imposed against LabMD?

A. They wanted a consent decree that wanted twenty years of biannual audits from an outside source at our expense. It would also open us up to additional penalties and/or fines.

MR. GORJI: Your Honor, I'm going to object. It's not something that -- negotiations are not something that would be held against the FTC at this point. There is an administrative complaint that's been filed, but a consent decree is a negotiation.

THE COURT: Well, have you offered -- have you shown them a consent decree with a proposal that that would resolve the matter?

MR. GORJI: There have been negotiations, Your Honor, in the past.

THE COURT: Well, is it -- would the FTC ever agree not to resolve this case without an ongoing consent decree subjecting them to monitoring over a long period of time, which is my experience with the FTC?

MR. GORJI: Your Honor, my understanding is that negotiations are no longer occurring. There is an administrative complaint and an ongoing administrative process that doesn't necessarily request the exact same relief.

THE COURT: Well, you can cross-examine him on that, and once the cross-examination is done, I will

determine whether or not that's something that would go into my consideration.

MR. GORJI: Sure, Your Honor.

Your Honor, if I may? I plan on handling the cross-examination, Ms. Fascett plans on handling the argument today, if that's all right with the Court?

THE COURT: That's fine.

MR. GORJI: Thank you.

BY MR. RAIDER:

Q. Is it your understanding that the fact that LabMD is merely archiving its records today would change the relief the FTC is seeking against LabMD?

A. No, it's not. That's not my understanding.

Q. Let's go back a step and discuss LabMD when it was providing cancer detection services in 2013 and the years before.

How much revenue did LabMD generate each year roughly?

A. It ranged between three and a half to seven and a half to eight million approximately.

Q. And how much revenue has LabMD generated in calendar year 2014?

A. Approximately fifty thousand dollars.

Q. And how much revenue has LabMD projected to generate in the second half of 2014?

A. Probably another fifty to seventy-five thousand

dollars.
Q. And how much profit did LabMD generate in the years it was generating millions of dollars in revenue?
A. With the exception of 2013, our profit margin was approximately 25 percent. In 2013 we lost approximately half a million dollars.
Q. How much profit has LabMD generated so far in calendar year 2014?
A. None.
Q. And looking to the second half of calendar year 2014, how much profit is LabMD expected to generate?
A. Zero.
Q. How many employees did LabMD have on its payroll in 2013?
A. Between 25 and 30.
Q. And how many employees does LabMD have today?
A. One.
Q. I want to shift topics again and talk a little bit about LabMD's insurance program.
A. Okay.
Q. What types of insurance did LabMD have when it was offering cancer detection services?
A. We had medical malpractice for the company, we had malpractice for the physicians, we had directors and officers insurance, we had general liability insurance, we had medical

insurance, dental insurance, workmen's comp and vision. I think that's everything.

Q. Which of these policies does LabMD currently have?

A. We have a COBRA for medical and dental, and that is all.

Q. In the years 2013 and before, what issues did LabMD encounter in obtaining insurance?

A. We never had problems getting insurance prior to 2013.

Q. Were you told why your insurance -- why LabMD's insurance policies would not be renewed?

A. Yes. Because of the -- the claims that weren't renewed, is was because of the FTC investigation, the ongoing cloud, and the fact that it involved medical records. So that even the policy that wasn't even covering a claim of that type was refused for that reason, meaning the medical malpractice insurance.

Q. And let me refer you to Exhibit 15 in your notebook.

A. Yes.

Q. And let me ask you some --

MR. RAIDER: Your Honor, I would like to show this to the witness and establish a foundation.

BY MR. RAIDER:

Q. What is this document?

A. This is an e-mail string from our broker that was sent to me between I believe our broker and one of his staff

members and an underwriter for OneBeacon Pro.

Q. And how did you receive a copy of this?

A. Because the broker sent it to me to show me that the company wasn't going to be interested in insuring --

MR. GORJI: Objection, Your Honor. Hearsay.

THE COURT: Is there any objection to this e-mail?

MR. GORJI: Your Honor, I can get into it on cross.

THE COURT: Pardon me?

MR. GORJI: I can get into it on cross.

THE COURT: So is there any objection to the introduction of the e-mail?

MR. GORJI: No, Your Honor.

THE COURT: It's admitted.

BY MR. RAIDER:

Q. Who is Mr. Coscarelli?

A. Mr. Coscarelli is an underwriter at OneBeacon Pro who communicated with my broker.

Q. Who is Mr. Seilkop?

A. Fred Seilkop is the owner of -- I believe of Healthcare Professional Services and my broker.

Q. And who is Ms. Garrido?

A. Betsy Garrido is an assistant that works for Mr. Seilkop at Healthcare Professional Services.

Q. What insurance policies are being discussed in this e-mail thread?

A. This is the facility, what we call tail coverage or ERP, which is extended reporting period coverage. After a practitioner, a medical facility, ceases practicing their operations in that manner, then you have to get coverage to extend any claims that come for that reporting period where they were working there.

Q. What reason is Mr. Coscarelli offering for declining to offer insurance to LabMD?

A. He says, The potential volatility due to the FTC investigation is something we want to stay away from, particularly because it pertains to medical records.

Q. Has LabMD been able to obtain an offer for an extended reporting period after January 2014?

A. I split the search. We had almost everyone say no.

I did have -- I found a company in Florida who offered tail coverage to the physicians, so I split them off and got their own tail coverage, and we don't have any medical coverage, medical malpractice coverage.

Q. You mentioned having comprehensive general liability insurance. What is the status of your efforts to renew that policy?

A. They nonrenewed effective May 5th of this year -- that was Hartford -- because of the Federal Trade Commission claims history.

Q. And what impact does that have on LabMD's ability to

offer cancer detection services?

A. Well, to offer cancer detection services, you obviously have to have a facility where you can offer that, and we are required to have general liability insurance in our facility and under our lease or anywhere else where we want to open up space.

So without being able to get general liability insurance, we can't function.

Q. I want to switch topics again and talk a little bit about the regulatory oversight of LabMD as an ongoing provider of cancer detection services.

Separate from the FTC, was LabMD subject to government regulation?

A. Yes.

Q. By whom?

A. By the federal -- the U.S. government and the State of Georgia under CLIA and DHR has a -- there is a laboratory oversight group within the Department of Human Resources in the State of Georgia.

Q. And in years 2013 and before, how many times has HHS raised concerns about LabMD's compliance with HHS regulations?

A. We never had a problem.

Q. And what about as to the State of Georgia?

A. No, no problems.

Q. If you could turn to Exhibit 23 in your notebook?
A. Okay.
Q. What is this document, just at a high level so we can get it introduced into evidence?
A. It is a -- we are required to submit specimens to an independent source that reports to the government our testing and accuracy, and so that's what that is.
Q. Is this a business record of LabMD?
A. Yes, it is.
MR. RAIDER: We tender this into evidence, Your Honor.
THE COURT: Any objection?
MR. GORJI: No objection, Your Honor.
THE COURT: It's admitted.
BY MR. RAIDER:
Q. What does it mean to have a rating of 100 percent compliance?
A. That means that all the tests came within 100 percent of the acceptable range of the independent agency on the testing -- on the results we reported. So it's an accuracy of test reporting reports.
Q. The certificate indicates a November 2013 expiration date. What was the status as of January 2014?
A. I'm sorry, can you point the certificate out? I'm not seeing it.

Are you on 23?

Q. Yes. I'm looking at the --

A. I'm on a different 23.

Q. -- expiration date on the right?

A. My 23 is not the same as your 23.

THE WITNESS: Can he show me --

THE COURT: This is not my hearing. This is your lawyer's.

THE WITNESS: Okay. That's my 23.

THE COURT: Why don't we do this. Since you have three other lawyers here with you, maybe they could find this for you and we can move on.

MR. RAIDER: Okay, we will.

MR. GORJI: Your Honor, I would also like to make sure the government has the correct 23 as well.

MR. RAIDER: Yes. I apologize for that.

THE COURT: My understanding is that Exhibit 23 is a one-page document that is sent by the American Proficiency Institute and it's dated March 5th of 2014.

MR. RAIDER: Yes.

THE COURT: Is that Exhibit 23?

THE WITNESS: No.

MR. RAIDER: That's what we are asking to have admitted.

THE COURT: Well, that one-page document has been

admitted.

MR. RAIDER: Yes. And I will move on.

BY MR. RAIDER:

Q. You said that HHS has not raised any concerns about LabMD's compliance with HHS regulations. What issues specifically, if any, has HHS raised concerning LabMD's data security program?

A. None.

Q. Has HHS launched an enforcement action against LabMD because of concerns over its data security program?

A. No.

Q. Have they, to your knowledge, instituted an investigation?

A. No.

Q. Have they issued notices of violation or documents to that effect?

A. No, sir.

Q. Okay. I want to switch topics one more time and talk about your website and your blog.

Have you created a blog?

A. Yes.

Q. And what is the website that hosts that blog?

A. *MichaelJDaugherty.com*.

Q. And on your blog, have you posted opinions about the FTC?

A. Yes, I have.
Q. And could you describe what you have said about the FTC?
A. I have -- I'm very opinionated about the overreach and lack of standards for rules or clarification and yet still the exhaustive investigation. So I have posted what I consider to be my opinion and First Amendment right speech about how they have conducted themselves throughout this.

Because we have never known what we have done wrong, and that's been a huge frustration, and it's so damaged the organization that I have spoken about that in several blogs.

Q. In your dealings with FTC employees as part of this LabMD enforcement action, what did you perceive to be the reaction to your blog posts criticizing the FTC?
A. My perception is that they are very upset and unhappy about it. They don't like any public criticism.
Q. Is it your opinion that the FTC has retaliated against LabMD because of your blog criticizing the FTC?

MR. GORJI: Objection.

THE COURT: Overruled.

A. Yes, it's my opinion that they retaliated.
Q. Has the FTC monitored your website with the blogs?
A. Yes, they have.
Q. Okay. I want to discuss Google Analytics. What is

Google Analytics?

A. Google Analytics is a tool provided by Google to analyze the traffic and effectiveness of --

MR. GORJI: Objection, Your Honor, to the basis for his knowledge. There is no foundation here. He does not work for Google.

The attachments that he's provided to his declarations he has no basis for authenticating. We are objecting on those grounds, Your Honor.

THE COURT: Are you denying that the FTC has monitored his blog?

MR. GORJI: No, I'm not denying that. But, Your Honor, the specificity of representations made in the declaration have no foundation.

THE COURT: All right. Well, maybe we could bring somebody in from Google and extend this hearing, if you would like.

It seems odd that if you are an enforcement regulatory body, that rather than doing your regulatory activity, that you would be monitoring somebody's blog that is criticizing the FTC, unless you are thin-skinned about that.

MR. GORJI: Your Honor --

THE COURT: You have just acknowledged that the FTC is monitoring his blog. Are you doing that in connection

with your regulatory investigation or are you doing that for your interest in his company and what they are saying about it, about the FTC?

MR. GORJI: Your Honor, the government and agencies monitor individuals' websites on a routine basis. In addition, here, Your Honor --

THE COURT: Why?

MR. GORJI: To determine whether or not there is any information that they might be able to add to their case.

THE COURT: So are you doing that in connection with your regulatory activities and responsibilities in connection with this investigation of LabMD?

MR. GORJI: Your Honor, I would have to confer with the FTC officials on the exact reason. I haven't been provided an exact reason.

And, again, the suggestion that it's for retaliatory purposes is purely speculative. There hasn't been any --

THE COURT: Well, under the Federal Rules of Evidence, somebody who has an experience that would provide a foundation for an opinion is admissible as a lay opinion.

He has now gone through this investigation beginning with the FTC's investigative activity beginning in 2010, which is now four years ago, and it would seem to me

that if he is able to establish when he began these public criticisms of the FTC and compare that with the investigative activity of the FTC and its various responses to actions that he's taken, that he could reach an opinion about whether or not he believed it to be or that it was his opinion that they were acting in a retaliatory manner, and, therefore, I'm going to overrule the objection.

MR. RAIDER: Your Honor, as to the specific reports, I just want to make clear that those also, I mean, if we establish a foundation, they would be admissible at this point. Is that part of your --

THE COURT: Probably not through him.

MR. RAIDER: Well, we would argue under Federal Rule 807 that there is sufficient reliability, that this is a service Google makes available to website owners to pull down information about traffic on their website.

THE COURT: Yeah, but the question would be the reliability of the information being provided by Google, and I don't think he has a basis to express that opinion.

MR. RAIDER: Understood, Your Honor.

BY MR. RAIDER:

Q. Just to go back and make sure, what is Google Analytics?

A. Google Analytics is a service or/and a tool that Google provides to website users, owners, to analyze and pull

reports down from Google's data of who is looking at the website, how long they stay, how deep they go, who they are, and so you can -- as a website owner, you can assess the effectiveness of reaching the audience you want to reach and you can see what audience you are pulling in.

Q. Have you generated website visit reports for your web -- for your blog post website?

A. I have, yes.

Q. What type of reports did you generate?

A. I generated the reports that would show who the top users were and what dates they were on and what ranges, and coincided those to some blog posts.

Q. What type of blog posts were you focusing on?

A. Well, as an example, there was a blog post when I first really announced that the FTC was suing me, which came out approximately September 17th, 2012.

And while I noted the Federal Trade Commission up until September 1, 2012, had never looked at my site one time, on that day or approximately that day or the day after the Federal Trade Commission had looked at that blog 75 times.

MR. GORJI: Objection, Your Honor. Again, there is no reliability for this testimony.

THE COURT: Is that true, that after this blog post, that there were 75 hits by the FTC in response to his criticism?

MR. GORJI: I don't know the answer to that, Your Honor. I haven't --

THE COURT: Will you find that out for me? Will you?

MR. GORJI: Your Honor --

THE COURT: Will you find that out for me?

MR. GORJI: I could contact Google and have FTC experts --

THE COURT: Why don't you contact your agency and find out if anybody in response to a critical blog post 75 times the next day accessed the blog?

MR. GORJI: Well, Your Honor --

THE COURT: And explain to me what was on the blog post that was of interest to your investigation of this company.

MR. GORJI: Your Honor, one --

THE COURT: Will you do that?

MR. GORJI: I can have FTC provide an explanation for that.

Your Honor, one aspect of this case is that there is retaliation, and in order to demonstrate retaliation, there has to be that his freedom of speech has been adversely affected. So it would make sense, Your Honor, for the government to continue to monitor whether or not he's still continuing to express his speech.

And I believe he is still effectively expressing his speech, and, therefore, there is a legitimate reason.

THE COURT: Are you telling me as an officer of the court that after a critical blog post, that somebody at the FTC, in order to make sure that he was -- that he was not impeded in his First Amendment rights, decided the next day to 75 times make sure that the same post was up there and, therefore, it could come in and make an argument like you have just made, that the purpose of that access was to make sure that he was unimpeded in the exercise of his First Amendment rights?

MR. GORJI: Your Honor --

THE COURT: Is that what you are saying?

MR. GORJI: Your Honor, that is not the sole explanation.

THE COURT: Is that what -- is that one of your explanations?

MR. GORJI: I believe that is a legitimate reason for --

THE COURT: And is that why the -- is that why you are representing to me that the FTC accessed his blog, was to make sure that his First Amendment rights were not being impeded?

MR. GORJI: No, I'm not making that representation, Your Honor, that that is the sole reason.

THE COURT: So you are backing from what you just told me?

MR. GORJI: No, no, Your Honor. I believe that one legitimate basis for --

THE COURT: Was that a legitimate basis on behalf of your client, the FTC, the reason why they accessed the blog post 75 times the day after the post was made?

MR. GORJI: Your Honor, I would have to get FTC to provide an explanation as to why they accessed it. I can --

THE COURT: You just told me twice that's one of the reasons they accessed it. Is that one of the reasons why they accessed it?

MR. GORJI: Well, Your Honor, I know that's one of the reasons why I accessed it, for example, during the course of this litigation.

THE COURT: Did you access it on September 17th or September 18th?

MR. GORJI: No, Your Honor.

THE COURT: How many times have you accessed it?

MR. GORJI: Maybe a handful, Your Honor. But -- and that was my motivation.

But I can also surmise, Your Honor, that a government agency might think that there is possibility of statements related to the conduct -- to the conduct that FTC is trying to regulate on his postings and looking for that

reason.

Now, whether or not that is the actual motivation here, Your Honor, I can't attest to that. I can ask FTC to provide you with their explanation.

THE COURT: This is taking an interesting and troubling turn which I never expected, for an admission by an FTC lawyer that they monitor blogs routinely of companies for whatever purposes, and you don't even know the purposes except for this purpose, that the only purpose that you have expressed, which I find incredible, is that you stated on behalf of your agency that the day after this blog posting was made, that the 75 times -- assuming that's true, but even if it was seven times, that they monitored it to make sure that his First Amendment rights were not being impeded, is incredible.

MR. GORJI: Your Honor, that's not my sole explanation. My other explanation --

THE COURT: But it's one of your explanations, isn't it?

MR. GORJI: Your Honor --

THE COURT: Isn't it?

MR. GORJI: Your Honor, I think perhaps that is probably an explanation as to why I personally did it. With respect to the FTC, I don't know whether or not that motivated --

THE COURT: Was my question unclear about the accessing of the website the day after the posting? Did you not understand that?

MR. GORJI: Your Honor, your question was not unclear. I perhaps was confused, but not because of the lack of clarity of your question. I apologize to the Court.

Again, I can have the FTC provide an explanation as to why they are monitoring, and my explanation is again what I surmise, but it may not be sufficient here. And, Your Honor, if Your Honor would like, we could have FTC provide an explanation to the Court.

THE COURT: Well, let's have this rule between you and me at least. This is a hearing. I am a judicial officer, and you are an officer of the court. When I ask you a question, don't duck and cover the question. Answer the question so that I know that what you are telling me is accurate and I can rely upon it. Is that fair?

MR. GORJI: That's fair, Your Honor. I didn't intend to give the impression that I knew what the reason was. I was providing an explanation as to why I think it might be reasonable.

THE COURT: Well, that's not what you said, and the record will be clear that in answer to my two questions, that is not what you said.

MR. GORJI: I apologize.

THE COURT: Instead you were coming up with a defense for the conduct. And that's a problem that lawyers have when they are unarmed with the facts.

MR. GORJI: I agree, Your Honor, I do not have the facts with respect to what their specific reasoning was.

THE COURT: Then the next time you answer a question, tell me that.

MR. GORJI: I apologize that I gave a misimpression to the Court, Your Honor.

THE COURT: Well, that's not a misimpression. You apologized for making an inaccurate statement in response to a question from the bench.

MR. GORJI: I apologize, Your Honor.

THE COURT: Thank you.

BY MR. RAIDER:

Q. Mr. Daugherty, if you could turn to Tab 31. Hopefully these numbers are correct.

A. I'm at 31, sir.

Q. Are those the Google Analytic reports that you generated?

A. Let me just review them, please.

Yes, sir. I believe those are all of them, yes, sir.

Q. And did you generate those reports?

A. Yes, I did.

Q. And how did you go about generating those reports?
A. I just signed onto my account or my password and ID that's hooked up to the website and started using the tool.
Q. I want to turn to the report. And I have the single pages in my notebook, unfortunately. I'm not sure how far into the exhibit it is. January 1 --
MR. RAIDER: Well, Your Honor, we tendered these reports for Mr. Daugherty to explain the information on them that he received.
THE COURT: So what does that mean, tendered to what?
MR. RAIDER: We would like to admit these reports into evidence.
THE COURT: Any objection?
MR. GORJI: Again, Your Honor, the government objects based on reliability.
THE COURT: Sustained.
BY MR. RAIDER:
Q. Was there information posted to your blog website that would shed light on the adequacy of LabMD's data security practices?
A. No, sir.
Q. Were you surprised by the number of times the FTC visited your website?
A. Very.

Q. Was there any reason that you are aware of why the FTC employees would have to view your blog website so many times?

A. As involved the investigation, no.

Q. I want to switch topics one last time. What is LabMD asking from the Court?

A. We are asking the Court to stop or pause the investigation so that we can try to recover from the cloud and loss of business revenue and loss of employees and loss of insurance and loss of reputation and revenue and we can try to start to recover.

Since they don't have standards and rules and won't tell us what we have done, they just point to consent decrees that say no wrongdoings in them and we have -- we just have -- it's been ongoing for years of not knowing what we are supposed to do or what we did wrong, and we have just been torpedoed.

Q. If the Court were to stop the FTC's enforcement proceedings against LabMD, would you restart the business to begin offering cancer detection testing services?

A. It would -- I would start the attempt to. We can't get insurance with this over our head. That's the first thing. And we have to -- and we are also being sued by the landlord. So we have a long stretch to get back.

And our key employees have left to other labs. Our

clients have left to other labs. Our landlord is suing us because we had to leave the lease earlier -- early. We have -- the insurance is not there.

And all that healing has to happen. So that will be able to start that, and also prevent us from going deeper in the hole by having no longer -- no longer having access for the physicians for the records they need now, which are required by us to keep, depending on the record, from five to ten years.

MR. RAIDER: Thank you, Mr. Daugherty. I have no further questions.

THE COURT: All right. Cross?

MR. GORJI: Yes, Your Honor.

-- -- --

CROSS-EXAMINATION

BY MR. GORJI:

Q. Good morning, Mr. Daugherty. How are you?

A. Good morning.

Q. I have got a question about the investigation and your speech. You agree that the investigation was already underway before you started critizing the FTC's conduct here?

A. Well, in January of 2010 they started a nonpublic inquiry. If you consider that an investigation, yes.

Q. And you began your criticism in early 2012; is that

correct?

A. My public criticism?

Q. Yes, your public criticism.

A. That was my blog. Yeah, I think the public criticism started with the *Atlanta Business Chronicle* interviewing me, and I believe that came out in September approximately 7th of 2012.

And that was because I had to do it because the Federal Trade Commission had filed suit for me to -- let me think. Let me just think here.

I mean, in August of '12, I believe that's when they sued for the CID, and that's when people started noticing and contacting me. Up until that point no one had known and I hadn't told anyone. But I was really forced to respond at that point.

Q. And your understanding is that the company Triversa found information about your patients, your customers? That was in 2008, is that correct, that you learned of Triversa finding that information?

A. Tiversa was contacted -- contacted me or my company LabMD in May of 2008.

Q. And the CID, the subpoena for information and documents from FTC to your company, that was in December 2011; is that right?

A. I'm sorry, yeah. You know, that's why my memory -- I

believe they filed the CID in December of 2011, and then the Department of Justice filed in August of 2012 to have the Court decide whether I had to sit for a CID.

Q. So your public criticisms began well after the CID was served on the company; is that right?

A. Well, it didn't -- the CID service from 2012 -- 2011, I, believe that was. Okay, I'm getting my years mixed up. Yes, yes.

So '11 they served right at Christmas, and no one picked it up publicly. And then when the DOJ I believe filed to have the Court decide whether I was required to, that's when the public started to come to me. That was the first time. So that's --

Q. So just so we are clear, and without focusing on dates, the CID came first, and then you started publicly criticizing?

A. Yeah, the CID -- I mean, yeah, the CID came in December 23rd, 2011, and the criticism was in September 2012.

Q. During the course of that time frame, between the CID coming and your public criticism, were there any depositions that took place with respect to employees of your company? Were there any other investigative things that occurred that impacted your company before you started publicly criticizing?

A. Well, yeah. The Federal Trade Commission was repeatedly

demanding more and more and more and more information, totally side-swiping my management team. Because we were in a house of mirrors, never-never land, not knowing what they wanted, and they wouldn't tell us what we did wrong, and it was relentless.

So it was -- and you are talking a company of like thirty people that diagnose cancer with one VP of operations.

Q. So the FTC was actively investigating before you started your public criticism?

A. Yes.

Q. I want to draw your attention to the FTC administrative complaint. Have you had a chance to look at that document?

A. Can you refresh my memory or bring it to me, please?

MR. GORJI: One moment, Your Honor.

THE WITNESS: I assume I can close this?

MR. GORJI: You should have it --

THE WITNESS: Oh, it's in the book?

MR. GORJI: You should have it as your Exhibit 8.

THE WITNESS: Okay.

BY MR. GORJI:

Q. Okay. Are you familiar with this document?

A. Yes, sir, I am.

Q. Okay. To date, has the FTC ordered you to do anything that would change your business conduct with respect to

managing patient-protected information?
A. No.
Q. Now, in your verified complaint in your declaration, you say that the cause of your company having to essentially wind down its business is a result of the FTC investigation?
A. That's correct.
Q. But it's not a result of anything that FTC has actually ordered you to do with respect to how to manage your patients', customers' protected information, is it?
A. We would have liked to have known that long ago. No, we haven't gotten that answer.
Q. Would you say that that is the primary reason why?
A. Yes.
Q. Have you ever given a contrary reason as to why your company had to wind down?
A. Contrary?
Q. Yes.
A. I have given additional. I wouldn't say contrary.
Q. What reason would you say?
A. I said that the Federal Trade Commission set the stage for our having to wind down operations because as a small company this was an overarching fishing expedition that never gave us standards, rules, reasons, and that just unspeakably slowed down a cancer detection center.
Because we only have so much energy, and so we had to

focus on this, and the only answers we were getting back was look at this consent decree, which was vague at best with fine print about no wrongdoing is admitted.

So we were in a never-never land. So we had to shoot -- we don't know where we had to shoot, so we felt the only way to get in a safe place would be to shoot for perfection.

So I had, you know, the management staff, especially the IT and my VP of operations, just spending so much time on that, and that energy was taken away from prepping for what we knew what was coming, which was Obamacare.

And so when we had plans to go into molecular science or into breast pathology, we couldn't get off the ground because we were getting diverted over here.

Because as a cancer detection center in a niche market, you specialize in just one area, and the expertise is just -- or the differentiation in the market is our expertise by our pathologists because they just read that kind of cancer, and that is something that physicians around the country want and patients benefit from, because practice makes perfect.

With Obamacare it was coming that that priority was fading away, and we were aware of that, and we were going to have to diversify our base.

And the Federal Trade Commission tied our feet together. We only have so much energy and time, and it was just overpounding for this small company.

So I have said several times that the Federal Trade Commission set the stage during this time so that we could not function and deal with what came with Obamacare.

And then with four weeks' notice due to sequestration, which usually it's more, we found out that our 2013 reimbursement was cut 30-something percent for pathology, and we started bleeding cash like crazy. And we were just so overwhelmed. It was like too many spinning plates.

And so -- and then that's just -- that's just the business model. Then you go into the specific knowledge that the VP of operations especially had and the IT guys, and really just how the fear and the unknown and the uncertainty, and eventually it just wore them down, and my VP left and he moved to Denver in August. And when that happened, that was just it.

And so we started losing, losing money. And then by -- I didn't want to ruin everyone's Christmas, but around December I knew this is just not looking good. It was just reality. We just were overwhelmed with reality.

So the FTC is not going away, we are not going to get more money, our reputation has been hashed, people that are employees are just afraid and so they are just leaving. And I couldn't give answers.

And so, you know, the ship just went down.

Q. Well, how would you say Obamacare itself impacted your

business?

A. Because CMS starts cutting costs for costs containment, and ancillary services went first. And so, you know, for cost containment those fee schedules were cut.

Q. And how about customers that you previously had, were they going to be referred to you for services under Obamacare?

A. Well, no, because what happened was what Obamacare does is it really forces a marketplace consolidation, and so physicians in the short term to survive were going to have to -- the physicians that we had -- I mean, this is not all physicians, period. I mean, this is just urologists and office-based urologists. So that's another reason why we've got to diversify.

But they were forced to either -- they either get huge and merge together, they either sell their practice to hospitals, or they retire.

And so we saw people having to basically survive for a consolidation reason, and so the purchasing -- you know, we knew that physicians were going to have to have economies of scale, so we were going to have to broaden who our customers could be to be able to get enough customers to survive because reimbursement was going down.

Q. So as a result of Obamacare, you lost a considerable amount of business?

A. No, we didn't -- well, we didn't lose business. We lost the revenue for the business we performed, and we were prevented because of the FTC action from building the business to survive. We could only handle one tidal wave at a time. We had two coming at us.

Q. Well, isn't it true that physicians and customers were not -- under Obamacare were no longer going to be able to refer to you for services?

A. In the urology marketspace, no.

MR. GORJI: One moment, Your Honor.

Your Honor, at this time I would like to cross-examine Mr. Daugherty with material that comes from the FTC administrative proceedings. It involves a deposition transcript.

Under FTC regulations it is protected and confidential, but there is a provision under the regulations that allows for its disclosure provided that we give notice. We did so last week, Your Honor.

But because it was previously confidential, I would like to give counsel an opportunity to take whatever measures they think necessary before I present it in open court.

THE COURT: And is this related to his direct testimony?

MR. GORJI: Your Honor, it addresses specifically whether or not Obamacare was the cause of loss of revenue and

the winding down of the company.

THE COURT: It is being offered as a prior inconsistent statement?

MR. GORJI: Yes, Your Honor.

THE COURT: So, Mr. Raider, what do you say about that?

MR. RAIDER: Your Honor, we would ask that a protective order apply and it be sealed at least for now until we see where it's going consistent with its status in the administrative proceeding.

THE COURT: I mean, can you introduce as a prior inconsistent statement a statement that you elicited in his examination?

Because he didn't say anything about Obamacare on direct examination. So you elicited the explanation on cross regarding Obamacare, and now you want to impeach the statement that you elicited with a prior inconsistent statement? And if so, how can you do that?

MR. GORJI: Well, Your Honor, he testified on direct that FTC's actions are the reason why his company had to wind down.

I asked him here whether or not he believes Obamacare is what caused it, and he says no, but I would like to point him to his testimony where he says the opposite in a deposition, sworn statement.

THE COURT: I know, but it's still testimony that you elicited on cross, and now you want to -- can you offer a prior inconsistent statement to rebut a statement that you elicited?

MR. GORJI: Your Honor, I think I can impeach him if he says something that's inaccurate. I can't bring in rebuttal evidence, bring somebody else in to impeach him, but I have a deposition, a sworn deposition.

THE COURT: Right. So what's your authority for that? Since you have been laying in wait to do this, so you must have a case or two for me to support the admissibility of --

MR. GORJI: Your Honor, I do not have any case law with me, and I wasn't at this moment seeking to introduce the exhibit. I was simply seeking to make use of it in open court to contradict the testimony here.

THE COURT: And do you have any authority that this protected material that I assume you got through this deposition under these circumstances should be allowed?

MR. GORJI: Your Honor, there is a provision, a regulation, 16 CFR Section 410 (g), that allows for its use upon notice to the party who has given the testimony in the deposition.

THE COURT: Of course, nobody ever told me you had done that. I had no idea this was coming up. I would like

to say I'm a pretty diligent fellow, but because nobody told me about these regulations, I will admit I haven't gone to look at them and I haven't memorized them.

So I do like to make careful rulings, and, you know, maybe there is another way of doing this, that you could submit after the hearing those portions that you claim are prior inconsistent statements, and the lawyer for LabMD can weigh in on whether or not it is or not, and then I can consider it after that.

But it seems to me fundamentally unfair that, one, you knew this was coming; two, you don't have any authority for me; and that you now want to disclose because you have given notice in this very public setting something which I think you know is not going to be favorable to this man individually and reputationally and in the lawsuit.

MR. GORJI: Your Honor, we did provide notice last week that we were going to make use of this transcript, so it wasn't trying to ambush anybody here.

THE COURT: Well, make use of it? Did you tell them in what specific way?

MR. GORJI: Actually, our filing from last week indicated that it would be to cross-examine him.

THE COURT: For whatever happens to be in that, without focusing on specifically what it is that you were going to use it for?

MR. GORJI: Well, we didn't identify the specific topic.

THE COURT: But you knew that's the topic that you were going to use, didn't you?

MR. GORJI: Yes, Your Honor.

THE COURT: Did you even have a communication with opposing counsel to say, look, this is why we want to use it, we don't -- our contention is that there were various and sundry reasons why the business failed, and we have this and you were there, and I just want you to know with respect to this notice that that's the purpose?

MR. GORJI: Your Honor, I didn't believe that providing an additional layer of specificity as to exactly what from the transcript we were planning on using was something that was necessary, and in light of the fact that we told them we were planning on using it and that would alert them as to whether or not their confidentiality interests were going to be implicated, the use of the transcript or not, not what the specific content of what I was about to say in court would implicate --

THE COURT: Let me just make this observation. There is a lot of acrimony in this case, and that impedes the sort of professionalism that I expect at a hearing that allows me to make a decision on a motion. I believe that that is impeding and affecting your judgments as to the

fairness of this hearing.

And, you know, I preside over very difficult criminal cases all the time where people's liberty is at stake, and I find more cooperation between lawyers in those on much more difficult issues, including evidentiary issues, than I see in this proceeding, which is the government coming in, which -- and I think it's the responsibility of the government to be fundamentally fair to the people that it's regulating, and that it would be in your interest and I would hope your motivation as an employee of the government to say here is what -- here is our position, here is how we are going to advocate it, because we want the Judge to have a clean record to make a decision.

So your explanation that you didn't think the additional level of specificity may be technically correct -- I don't know, because I haven't looked at the -- at what the requirement is with respect to disclosure -- but I will say this, it's now interrupted the proceeding, it's made it more difficult for me to understand the position of the parties, and I think it abrogates your responsibility as an employee and representative of the United States government and particularly this agency.

But that's sort of the theme I see in this whole investigation.

MR. GORJI: Your Honor, if I may address that? I

apologize if that is what has occurred in this case.

THE COURT: You know what my mother used to say? My mother, bless her heart, who is now dead, used to say when I apologized, she said you can't live a life of I'm sorries. Now you are living through a hearing of I'm sorries because this is now your third apology.

But it comes from the fundamental refusal of you and your colleagues with candor and with transparency to say here is where we are going on this.

Your whole position on this is that I don't have jurisdiction to do this, and that has -- and that's all you briefed is that I am not authorized to review the authority of your agency under Section 5 to conduct this investigation.

And so you are relying upon those what you think are bright line rules about a section, which in my course of doing this for for ten years is fairly ambiguous to me. But this is the first time where it hasn't been a direct consumer action, and I frankly think there is a legal question.

Now, the question for me is whether or not I have the authority to decide that or whether there is some other process that has to first be exhausted or however you want to advocate it through in order to get a final opinion that can be appealed to a court.

MR. GORJI: Your Honor, the jurisdictional arguments are the primary arguments we do make. We do also make the 12 (b) (6) arguments, Your Honor, that do not deny your authority but that we believe the causes of action fail to state a claim.

But I would just like to put something in perspective on behalf of the government here, Your Honor, which is the history of acrimony that you perceive, this is a case that I was just very recently assigned to along with co-counsel here. Counsel who was on this case is no longer with the Department of Justice.

And so I just became aware of this transcript last week, Your Honor. And so there certainly wasn't any --

THE COURT: That's not the defendant's or my fault or my problem. That's your problem. If you want to switch lawyers, you switch lawyers.

And if you are talking about the fellow who was here on the CID, I could tell you as a result of that hearing that there was already a history of acrimony and I think on behalf of the agency the exertion of authority in a mean-spirited way.

MR. GORJI: Well, Your Honor, I can just say that --

THE COURT: And you might -- you know, I'm not saying that -- if you are just new to this case, which

I think is the reason why I put this off, to allow you time, that I would hope that change in lawyers would change atmosphere.

MR. GORJI: Your Honor, there was no intention to hide anything from plaintiff here. We disclosed this in our filing, and, you know, if counsel had asked me what part exactly of the transcript are you hoping to make use of, I certainly would have answered that question.

THE COURT: Well, I know, but they are not used to you. They are used to the people who preceded you.

And it's hard for you to say this is a new day, and I suspect you didn't call them and say, look, we have got to change the atmosphere in this case, I understand that it hasn't gone well, we understand what your complaints are -- and I would hope that you would understand their complaints -- but we want to get on a platform that allows whoever hears this in whatever forum, that would facilitate the communication and entry into the record of information that would allow a thoughtful, just decision on a case that I think needs a thoughtful, just decision.

And I think especially when lawyers change, that it's the responsibility of the new lawyers to reach out and say we are going to handle this in the way that, one, advocates on behalf of our client, but at the same time, we recognize we are the government and we do want to be fair,

and we want to go down to Atlanta on this hearing that has been put off at our request, which I did because of people's personal commitments, and while my schedule is not very fluid or is not fluid at all anymore and it has very little capacity, it made sense to do that, and I did.

MR. GORJI: Well, we appreciate that.

THE COURT: But I expected this to go a lot better than it is.

MR. GORJI: Again, Your Honor, there was no intention to hide anything. By bringing the fact that we were going to use this transcript to counsel's attention, I thought that we had taken care of our obligations to alert them to the fact that we potentially --

THE COURT: Well, I don't know, because, one, nobody has told me what the obligation is, nobody told me that there was going to be a dispute about this.

And you didn't either, Mr. Raider. You were on notice. You didn't say, by the way, we are going to have a problem with that, let me give you a heads-up that that's going to happen. But you haven't said that.

In fact, I think you are kind of shooting from the hip to say, well, we don't want it to come in now, not even really understanding what they want to come in, even though there are four of you here today.

I hope you are not paying them all, because if you

are, no wonder you are going broke.

MR. RAIDER: Your Honor, the basic points, really, have already been made without the use of the transcript that --

THE COURT: Well, you know, this is -- you don't get to try the case for them, as much as you would like to.

MR. RAIDER: No, I'm not -- I understand.

THE COURT: The question is what -- and I don't want to waste any more time. We spent half an hour on this.

Is there some way for you to draw to my attention that would not disclose in this public forum information that you all agree at the time it was taken was deemed to be confidential or protected, that you could get whatever -- there can't be that much in this transcript that relates to that, that you could highlight those for me? And you can even do it today, and say here is what we would show him, and I would determine whether or not it is or is not consistent, and we can move on?

MR. GORJI: Your Honor, there really is only about two pages of text, and we could confer with counsel to decide if they are -- to come up with a proposal for Your Honor, if that's --

THE COURT: Why don't we do that now? Because I don't want this hanging over my head any longer than it has

been.

(Counsel confer.)

MR. RAIDER: Your Honor, we have no objection to the pages pointed out to us.

MR. GORJI: Your Honor, if I may approach the witness and provide him with this transcript?

THE COURT: You may.

BY MR. GORJI:

Q. Showing you your transcript from the FTC administrative proceeding on February 10th, 2014, it has your name on it. Do you recall giving testimony in that proceeding?

A. Yes, I do.

Q. And the attorney who asked the questions was Alain Sheer?

A. Correct.

Can you point out what testimony we are talking about?

Q. Yes, I'm going to draw your attention to page 130, line 25.

A. Can I read -- can I read this first?

Q. Yes.

A. What is the two pages? Can you tell me the beginning and the end, please?

Q. Yes, I am going to tell you. Starting on page 130, line 25, through 131, which is this page, line 12. If you would take a look at that?

A. That is the whole part of the two pages are these two things? Okay, so you don't mean pages of this; you mean transcript pages, okay.

Okay. So you are ending -- I'm sorry, you are ending on 131, line what?

Q. Line twelve.

A. Line twelve, okay. I'm sorry, thanks.

Okay, I have read it. Thank you.

Q. Was it your testimony there that you were asked, How does Obamacare fit into the decision to wind down LabMD?

Answer: It's creating huge anxiety, destruction, consolidation to our customer base.

Question: What does that mean for LabMD?

Answer: That means our customers are in survival mode and, therefore, are having to either sell their practices or merge with others and send their specimens to where they are told to send them, not where they want to send them.

Question: Is LabMD one of the laboratories to which your clients are told to send their specimens?

Answer: No.

A. Okay.

Q. Is it that your testimony there?

A. That was my testimony, yes.

Q. Also I'm going to draw your attention to page 60.

THE WITNESS: Okay. So did you look at this

additional? Okay.

BY MR. GORJI:

Q. I'm going to draw your attention to page 60 --

THE WITNESS: And my lawyers were okay with that other part?

MR. RUBINSTEIN: Yes.

THE WITNESS: Okay. Thank you.

MR. GORJI: I believe your lawyers do not object.

MR. RUBINSTEIN: No objection.

THE WITNESS: Okay.

BY MR. GORJI:

Q. I will point you to page 60, and if you start with line nine and go through line eleven?

A. Uh-huh.

Q. Was that your testimony there?

A. At that moment, yes.

Q. When you say that moment, that was on February --

A. -- 10th, 2014.

I mean, this is like out of context here, so let me just see what else is going on here.

Other than that, I don't know at the moment. It depends on -- other than that I didn't know at the moment, I didn't know the future plan -- I didn't know the factors of the future plan pertaining to Obamacare, and other than that, I didn't know other factors. I --

Q. So you agreed you were asked on line nine: What's your future plan for LabMD?

Answer: It depends on Obamacare, and other than that, I don't know.

A. And then, I didn't know what the future plan was. But I didn't say it was the only Obamacare. Okay.

Q. You can hold on to that.

A. Okay, thanks. Are we done for now? No? All right. Excuse me.

Q. Now, you mentioned that your VP of operations left the company?

A. Correct.

Q. Did he indicate whether or not Obamacare impacted his decision to leave?

A. No.

Q. And you haven't provided an affidavit from your vice president of operations, have you?

A. Well, he's no longer the vice president of operations.

Q. You haven't provided an affidavit from your former vice president of operations; is that correct?

A. You deposed him.

Q. You also claim that you have not been able to obtain insurance as a result of the FTC investigation. Did you inquire to the insurance providers whether or not it was the fact that there was an investigation or the fact that

customers' personal information was found in places that it shouldn't have been that gave them pause?

A. Well --

Q. Did you ask them that question?

A. I wouldn't have asked that question because that's an allegation about customers' information found in places other than it should have been. That's not a question I would have asked.

And whether that's true or not, when things are found in other places, that does not incite a government investigation. There are breaches that are hundreds of times greater than mine that have gone on, if mine had a breach, which we don't think it did.

So, no, that is not a question I would have asked. And because I was -- well, first of all, they won't speak to me directly. They tend to go through my broker. These insurance underwriters don't want to talk directly to the customer. They are going to go through the broker. So this is why the broker sent me the e-mail and conveyed information to me.

But according to the broker, it was the FTC investigation and the costs they are looking at. They are looking at risks and dollars.

Q. Certainly one of the risks that they would probably be interested in is whether or not your protected information is

adequately protected; is that correct?

A. No, because it's not a cyber security policy. They are interested in -- well, I would say they are interested in whatever can cost them, and whenever there is -- nothing scares an underwriter greater than the unknown or nothing scares a medical underwriter than a chronic disease.

And so I'm assuming since the only response that came from them -- and I didn't have direct conversations with them other than talking to my broker -- was that it was the unknown of the FTC investigation.

Q. Did you get an affirmative statement from the insurance company that they would cover you if the FTC investigation was enjoined?

A. No, I didn't.

Q. How many insurance companies have you contacted to obtain insurance coverage?

A. Well, I contacted brokers. They contacted insurance companies.

Q. Do you know how many insurance companies?

A. Approximately -- I think approximately a dozen, approximately. I am not quite sure. At least, at least seven or eight. But, you know, the brokers don't want to name names.

Q. And you don't have an affidavit from any of your brokers explaining why you have been denied coverage?

A. No, I don't have an affidavit from them.

MR. GORJI: One moment, Your Honor.

Nothing else, Your Honor.

Thank you, Mr. Daugherty.

THE WITNESS: Did you want this back?

MR. GORJI: You can keep it.

THE WITNESS: Okay. Thank you.

THE COURT: Any redirect?

MR. RAIDER: Just one quickly on redirect, Your Honor.

-- -- --

REDIRECT EXAMINATION

BY MR. RAIDER:

Q. Your deposition was February 10, 2014. What was the status of LabMD's cancer detection testing services on that date?

A. We were doing no more. That was about three and a half weeks out from our last report out.

MR. RAIDER: Thank you. No further questions.

THE COURT: All right. Thank you. You may return to counsel table.

THE WITNESS: Thank you.

THE COURT: Call your next witness, please?

THE WITNESS: Should I leave this here?

MR. RAIDER: Thank you, Your Honor. We call

Mr. Cliff Baker. And Mr. Meyer will handle that examination.

-- -- --

CLIFF BAKER

being first duly sworn by the Courtroom Deputy Clerk, testifies and says as follows:

-- -- --

DIRECT EXAMINATION

BY MR. MEYER:

Q. Mr. Baker, could you state your full name and address for the record?

A. Cliff Baker, 4850 Topeka Court, Dunwoody, Georgia.

Q. And where are you employed?

A. A company called Meditology Services based in Atlanta.

Q. In what capacity?

A. I'm the CEO and founder of the company.

Q. And what exactly is your role as the CEO?

A. Obviously oversee the running of the company, but I also lead a practice that focuses on privacy and security in healthcare, consulting with companies around privacy and security in healthcare.

Q. And when you say consulting about privacy and security, what exactly do you mean?

A. My career has been focused on helping primarily healthcare organizations adopt security practices that first

and foremost align with the security rule and then generally good practices to have a place to protect information.

Q. What were you asked to do in this case?

A. I was asked by counsel to review Dr. Hill's report and compare it to my understanding of the HIPAA obligations for companies in the healthcare industry.

Q. And what additional experience do you have to make such an analysis?

A. As I mentioned, I spent almost twenty years now helping organizations in the healthcare industry implement security controls to comply with HIPAA.

Prior to starting Meditology Services, I spent about fourteen years at a company called PriceWaterhouseCoopers primarily in the healthcare -- leading their healthcare security practice and consulting with their clients around implementing security practices.

After I left PriceWaterhouseCoopers in 2008, I was the chief strategy officer and architect for a framework called the High Trust Security Alliance, which essentially was a number of organizations across the healthcare industry that came together to try and define a reasonable and appropriate standard for the industry so the industry could proactively implement controls for the healthcare industry.

Q. And based on that experience, could you briefly state any opinions you reached regarding the standards articulated

in Dr. Hill's report?

A. The most troubling aspect of the report is that Dr. Hill doesn't take into consideration any aspects of scalability in terms of what's reasonable and appropriate for an organization of the size of LabMD to implement security to comply with HIPAA security requirements, which has really been the primary driver for security requirements for the industry.

And so when I read Dr. Hill's report, it is out of line with the expectations of organizations of the size of LabMD.

Q. Is it your understanding that LabMD is a HIPAA-covered entity?

A. It is my understanding that they are a HIPAA-covered entity.

Q. And based on your experience, do you have any reason to believe that the standard articulated by Dr. Hill would create confusion amongst HIPAA-covered companies?

A. Absolutely. The industry continuously is looking for clarification and specificity from the regulators to make sure that they understand what their obligations are, and when a regulating body makes a judgment based on some standard, the industry reacts and the industry tries to understand what their obligations will be as a result of that ruling.

So I think the position that Dr. Hill takes is

contradictory to the ten years of experience we have had with HHS and understanding their expectation of the industry.

Q. And following up on that, I want to go through some particular topics. What is scalability?

A. In the creation of the HIPAA rule, a key tenet of the HIPAA rule was to implement controls that were reasonable and practical for the resources, capacity, skills of an organization.

HIPAA recognizes that the healthcare industry ranges from large multinational companies to one-physician practices with no IT resources -- probably no IT resources on staff, maybe an office manager at best. And so HIPAA had to be able to specify requirements that would be adopted for the largest companies and the smallest companies.

Obviously specifying specific requirements for each of those extremes is difficult, and so HIPAA created this concept of a risk assessment which allowed organizations to analyze their exposures and to make decisions that related to the security controls that were appropriate and that they could really have the resource, capacity and skills to implement.

Q. And how does Dr. Hill address scalability?

A. Her primary considerations for scalability is the number of records that LabMD holds. And, candidly, the number of records at LabMD is minute compared to larger organizations

that offer similar services.

And then she doesn't really ever consider the type of organization they are in the industry, the number of employees that they have, the number of resources that they have hired from an IT and security perspective. None of those considerations come into her -- the basis of her opinion in her report.

Q. How significant is the difference between the standard Dr. Hill articulates and what HIPAA requires?

A. From my perspective, it's significant. Imposing requirements on an industry that are not practical and reasonable, you know, really have a contrary impact to what I believe the regulators are trying to do, which is to make sure that appropriate security controls are in place.

And so imposing requirements that don't address this kind of scalability aspect will distract the industry in large part because now they have to interpret and figure out how they are going to implement requirements that are misaligned with expectations that have been set for them for the past ten years.

Q. How important is scalability for a company the size of LabMD?

A. It's extremely important. Textbook security requirements or controls, if you read textbook requirements and you put the same requirements in front of a large

multinational company, you know, they have more security resources than LabMD has employees. And so the skills and investments that they will make around security would probably exceed the total revenue that LabMD probably pulled in its entire existence.

So it's incredibly important, because if the regulators want real controls to be implemented, they have to make them practical and they have to make them reasonable and they have to impose expectations that small organizations can actually achieve.

Q. What is integrity monitoring?

A. Dr. Hill refers to this concept called file integrity monitoring, and it is essentially technology used to monitor any change to files on an issue.

So it essentially looks for any change, whether you save a file or you implement a new file or put a new file on a computer, it will send off an alert to somebody. And somebody will have to read that alert, investigate it and respond to it.

Q. Does HIPAA require file integrity monitoring?

A. It doesn't specifically require file integrity monitoring at all.

Q. And what does Dr. Hill say in her report?

A. This is one of the key controls that she says LabMD should have had in place. And I think it's a classic example

of where her report is out of alignment with the expectations that HHS sets for the industry.

As an example, Dr. Hill often in her report refers to free software or inexpensive software that can be implemented to achieve some of these controls. What she doesn't consider is the resource requirements to follow up, investigate, configure, implement those tools.

And file integrity monitoring particularly has a significant resource impact on an organization because it's constantly sending out alerts that need to be investigated.

Furthermore, Dr. Hill recommends that file integrity monitoring be implemented on a workstation. So on occasion for large organizations you will see it on servers.

The reason I'm making that distinction is when a user is on a workstation, they are often changing files. You are opening Word documents, you are opening Excel documents, you are opening and closing files.

With that kind of software, there is a potential for an alert to be sent out every time a file is changed, and you can imagine the resource impact that that's going to have on the resources of a particularly small organization.

Q. For a company the size of LabMD, what would you recommend with respect to file integrity monitoring in order to be in compliance with HIPAA?

A. HIPAA is based on a risk assessment first.

Fundamentally HIPAA requires risk assessment. And so we'd work with a company the size of LabMD, understand their exposures, and essentially put a measured program in place to implement security over time.

We would start with some limited monitoring that would be in place probably on the servers versus their workstations and then evolve that over time.

The primary reason we would not start with file integrity monitoring is we know that it would overwhelm their resources and that the net impact would be that security would not be implemented, information would not be well protected because the resources would not have enough capacity to actually focus on the things that matter.

Q. All right. What is encryption?

A. Encryption is a process of turning readable information into unreadable information that is only accessible or unlocked for the individuals that have keys to unlock that information, in laymen's terms.

Q. Does HIPAA address encryption?

A. It does address encryption.

Q. How?

A. It's an addressable requirement.

And there is a distinction, an important distinction in the rule. There are required items and addressable items in the rule.

And HHS guidance for addressable items is that the decision around how to achieve those requirements, addressable requirements, should be based on the risk assessment, and then HHS essentially provides options.

If the organization does a risk assessment and believes that there is an exposure, believes that they have ways that cost and impact from a resource capacity on the organization in terms of implementing that control to mitigate the exposure, they should go ahead and do it.

On the other hand, in evaluating the exposure against the cost and resource capacity to achieve that control, if that cost and resource capacity exceeds the capabilities, they can explore alternate options.

If no alternate options exist, then they don't have to implement that control.

Q. What is Dr. Hill's opinion with respect to encryption?

A. Dr. Hill's opinion is pretty black and white, that encryption should be implemented.

Most troubling I think about her report is that she makes reference to encryption and risk. What I mean by that encryption stored in databases on servers.

And candidly, you know, across all industries, that is not generally an adopted practice, primarily because it has an impact on the processing speed and performance of systems. We are starting to see more and more of that kind

of control implemented, but mostly for large organizations that have the resource capacity to implement those kind of controls.

It's very unusual -- I have never seen an organization the size of LabMD implement encryption and risk.

Q. What would you recommend to an organization the size of LabMD with respect to encryption in order to comply with HIPAA?

A. Again, it would be based on the risk assessment, and I would recommend implementing controls where I know they can achieve the objectives required for encryption.

So for example, for any access to their website, if there was particular health information exchanged, I would expect that information is encrypted.

Q. You mentioned the risk assessment throughout your testimony now. Does Dr. Hill have an opinion regarding risk assessment?

A. She certainly does.

Q. And what is it?

A. You know, interestingly, we both refer to the same standard reference for risk assessment, which is the NIST Security Series Reference 800-30, which is a government-published approach for performing a risk assessment.

Where Dr. Hill and I have a departure in kind of

methodology, she immediately will go in her report to suggesting that the organization implement technical tools to achieve the risk assessment.

And again I think this is based on her experience in kind of, you know, she seems to have a very technically kind of focused career, technology focused career, and so her immediate response in terms of this risk assessment is to implement a number of technology solutions.

As I mentioned to you before, the license cost for those solutions may not be high. The resource cost to actually manage and implement those solutions is significant.

And when you look at the way HIPAA and HHS guides the industry in terms of doing a risk assessment, it's certainly not starting with implementing tools. It's with a process and a mind-set and a methodology, candidly mostly relying on manual methods to assess risk.

I think that kind of highlights the fundamental distinction between Dr. Hill's report and generally where HHS is guiding the industry.

Q. In offering those opinions, does Dr. Hill rely on any published materials from FTC?

A. She doesn't, which I found interesting.

I would have thought that the expert -- the expert witness for the FTC would have been referencing FTC guidance for security requirements. She did not reference that in her

report, that I recall.
Q. Are you aware of the FTC publishing data security standards for medical service providers other than what's in Dr. Hill's report?
A. I am not aware. In my line of business, I don't rely on FTC guidance for security requirements for my client base.
Q. And you have been in that line of business for almost twenty years; right?
A. That's correct.
Q. And in that time, are you aware of any statements made by the FTC expressing their authority to impose requirements on protected health information in excess of HIPAA?
A. I am not aware of those requirements.
MR. MEYER: No further questions, Your Honor.
THE COURT: I want some clarification to make sure, see if my understanding about this is correct. That -- and I guess this is an allegation.
The allegation is that the security breach here was the disclosure of certain patient records. And I don't know the quantity of the patient records that are alleged to have been disclosed, but apparently it was some patient information; is that right?
MR. RUBINSTEIN: Your Honor, Reed Rubinstein. If I might?
It's not clear. We have heard different things in

the course of the administrative hearing. Originally there was a focus --

THE COURT: Well, what's your understanding about what went from LabMD outside of the company to others, or are you claiming that nothing did?

MR. RUBINSTEIN: There are allegations that --

THE COURT: No, what's your understanding? Have you reached a conclusion that certain patient information was disclosed outside the company?

MR. RUBINSTEIN: Our understanding, based on the testimony that's been taken to date --

THE COURT: Well, you are the lawyers for the company.

MR. RUBINSTEIN: That's correct, but --

THE COURT: Have you reached any conclusion that information that was private for patients that was delivered to you by these people that were hiring LabMD got disclosed outside the company?

MR. RUBINSTEIN: We do not believe that information -- patient PHI has been disclosed outside the company based on what we have learned on discovery.

And the reason for that, among other things, testimony of the FTC's experts with respect to the expected rate of identity theft. In this case, there is no single plaintiff, no single person who has alleged --

THE COURT: All right. My question was do you know. You are saying there is not.

Second, did somebody load a file-sharing program on any LabMD computer?

MR. RUBINSTEIN: Yes.

THE COURT: And did you do any investigation to see whether or not any information was accessed through the use of that file-sharing program from somebody outside the company?

MR. RUBINSTEIN: I believe in approximately 2008, LabMD was informed that file-sharing software was on the computer. LimeWire, which is used primarily for audio files.

There was an investigation done by the company. This was contrary to the company's policies, and it was removed.

The FTC investigation began two years -- approximately two years thereafter, and there are allegations with respect to two specific alleged data breaches.

The first related to an insurance agent file, a 1718 file. A second related to certain day sheets, which were actually printed forms. They had nothing to do with data security in the sense that we are using it.

It is not clear to us still today and there is no evidence in the record that demonstrates how exactly the 1718

file, if it did, got out. That's one of the things that's still, frankly, developing.

But as I said, to our knowledge and as far as we can tell to the government's knowledge, there is not a single case of identity theft attributable to the alleged data breach.

THE COURT: Well, what is it that the FTC claims was the data security breach?

MR. GORJI: Your Honor, there are two instances, one being that the Sacramento, California, Police Department found information belonging to LabMD's customers in the hands of identity thieves.

Now, that was reported to LabMD. My understanding is LabMD actually informed customers that there had been a --

THE COURT: And when was that?

MR. GORJI: That was October 2012. I don't know when LabMD actually informed their customers or there was a disclosure.

THE COURT: And how did the police department know that it originated from LabMD, and in what form did they have it?

MR. GORJI: Your Honor, there was documentation that indicated it pertained to LabMD, I believe.

THE COURT: You mean papers?

MR. GORJI: Documents, papers.

THE COURT: All right. So -- and where did the police department claim that the papers -- how were the papers obtained?

By papers, you mean paper documents, that somehow they got hold of some paper documents with some patient information on it? Is that what the allegation is?

MR. GORJI: Yes, Your Honor. My understanding is they were in possession of the individuals who pled no contest to the state charges of identity theft.

THE COURT: Well, if they pled no contest, they probably cooperated. Did they tell you where they got the papers?

MR. GORJI: Your Honor, if I might inquire?

Your Honor, I don't have information as to how the documents and the information was obtained by the identity thieves.

THE COURT: Well, has anybody from the FTC gone out and interviewed the people who pled *nolo* to that to find out where it came from, to see whether or not there was indeed a security breach?

Let me tell you something, these are the most simple questions of this investigation. That you are claiming that some police department prosecuted some people for having possession of information which you are now

claiming wrongfully was not protected by LabMD, and you can't even tell me whether or not you have interviewed the people who had the data to find out where they got it to see whether or not there was a security breach or not? And yet you have implemented and instituted this investigation?

And this is your case. You are new -- I know you might be new on it, but for heaven's sakes, you are arguing to me that there is a hearing on May 20th and you don't even know.

MS. FASCETT: Your Honor, if I may just explain, just for clarity, not as an excuse. The FTC attorneys that are handling the administrative proceeding in that hearing, they I'm assuming definitely know these details. They are not present. They are not here today.

We are just -- we were just brought in from DOJ to represent this complaint in this action. So that's part of why we don't have these facts. But we represent the FTC here and we can get these facts for you.

MR. RUBINSTEIN: Your Honor, if I could?

THE COURT: I'm not --

MR. RUBINSTEIN: I --

THE COURT: Sit down.

MR. GORJI: Your Honor, my --

THE COURT: So where are those lawyers? Are they too busy to come to Atlanta today?

MS. FASCETT: Well --

THE COURT: Is that one of them sitting back there in the gallery?

MS. FASCETT: No, she's a U.S. Attorney here in Atlanta, unrelated.

THE COURT: How about this other fellow back there, is he an FTC lawyer too?

MR. MARCUS: Your Honor, we have a gentleman here from the FTC.

THE COURT: Are you involved in this investigation?

MR. MARCUS: I am personally not involved in the investigation.

THE COURT: Okay. So you are off the hook.

So far I have got four lawyers here and none of them are involved in the investigation. How about --

MR. MARCUS: We do have are a lawyer who is involved in the investigation.

THE COURT: And what's your name?

MR. SCHOSHINSKI: Good morning, Your Honor. Robert Schoshinski. I'm assistant director in the Division of Privacy and Identity Protection.

THE COURT: All right. So in this case, what investigation has been made as to the source of the documents that the police department out in California found?

MR. SCHOSHINSKI: Your Honor, the complaint counsel, so that is the FTC counsel who is litigating the complaint in the administrative action, noticed the depositions of the two individuals who pled no contest to identity theft.

One they could not serve because she was just simply not findable. The other one was in jail. We --

THE COURT: Did you try to find her?

MR. SCHOSHINSKI: Yes, we did, Your Honor. We hired several process servers. They made many attempts to try to find her but were unable to serve her.

THE COURT: And when did you first try to serve her?

MR. SCHOSHINSKI: Your Honor, I don't have the exact dates, but --

THE COURT: Well, give me an approximation.

MR. SCHOSHINSKI: Your Honor, I would say late 2013, early 2014.

THE COURT: So really late in the game, you finally decided that it made sense to go and find out with respect to one of the allegations that's the basis of your investigation that's been ongoing for months, because the CID was something I dealt with some months ago, that you finally decided -- or not you, but your lawyers finally decided that maybe it would be good to try to find the people who actually had the

information to determine where they got it?

MR. SCHOSHINSKI: Yes, Your Honor.

THE COURT: Does that strike you as odd?

MR. SCHOSHINSKI: Your Honor, it doesn't strike me as odd. It's what --

THE COURT: Does it strike you as late?

MR. SCHOSHINSKI: Your Honor, it strikes me as the normal course of the investigation.

THE COURT: Boy, that's a sad comment on your agency, that you would wait until months before a hearing and months after you instituted an investigation on a principal claim that you are asserting, that you have not even taken any effort to interview the people that you claim had the documents that underlie the charge of a security breach. That strikes me as almost being unconscionable.

And how much money -- how much activity was there before you served those subpoenas trying to get the information from LabMD with respect to a security breach that you don't even know how it occurred? How much activity?

MR. SCHOSHINSKI: Your Honor, how would you like me to estimate?

THE COURT: Let's start in months.

MR. SCHOSHINSKI: Well, Your Honor, I believe the investigation began in January of 2010.

THE COURT: Okay. So three years before you tried

to subpoena them?

MR. SCHOSHINSKI: Your Honor --

THE COURT: I'm sorry, two and a half years.

MR. SCHOSHINSKI: Your Honor, the knowledge of this incident didn't occur until after the CID enforcement hearing up here in Atlanta. That's when we were notified that this incident had occurred, in October of 2012.

THE COURT: So you found out about the -- the incident you are talking about is the California police incident?

MR. SCHOSHINSKI: That's correct, Your Honor.

THE COURT: All right. And how soon after you found out about the incident did you try to contact the police authorities in California to find out what they knew about the source of the information?

MR. SCHOSHINSKI: Immediately.

THE COURT: And what did they tell you?

MR. SCHOSHINSKI: They told us that they did not know.

THE COURT: And then what did you do next, and how soon did you do it?

MR. SCHOSHINSKI: We shared the information with LabMD concerning the -- what we found out once we were able to confirm that it was LabMD's information, and we then attempted to find out further from the California police

department what they knew about the source of this information.

THE COURT: And what did they tell you they knew about the source?

MR. SCHOSHINSKI: They told us they were not able to get the source from the defendants in the case.

THE COURT: Did you talk to the prosecutor of the case as well?

MR. SCHOSHINSKI: I don't believe so, Your Honor.

THE COURT: And so you tried to track down one of the two defendants. Did you try to track down the second of the two defendants?

MR. SCHOSHINSKI: Yes, Your Honor. We actually obtained service on the second defendant, who was in jail. We noticed his deposition in the action, went to take his deposition, and he pleaded the Fifth Amendment and refused to answer questions.

THE COURT: So sitting here today, you have no idea where the documents came from, whether they came from LabMD or some other source? Is that a fair thing to say?

MR. SCHOSHINSKI: No. We believe they were LabMD's documents.

THE COURT: Well, they might have been LabMD's documents, but you don't know how they got into the possession of the two individuals that you tried to contact

that pled guilty to this offense?

MR. SCHOSHINSKI: That's correct, Your Honor.

THE COURT: So you have no information to establish how those documents were obtained; is that right?

MR. SCHOSHINSKI: That's correct, Your Honor.

THE COURT: And you are still proceeding on this claim?

MR. SCHOSHINSKI: Yes, Your Honor, because the claim is not concerning that incident alone. It's concerning --

THE COURT: All right. But are you still proceeding on that claim?

MR. SCHOSHINSKI: We are proceeding on that evidence, Your Honor.

THE COURT: And that evidence relates to other claims, because you have other documents that were found in other places?

MR. SCHOSHINSKI: That evidence relates to the potential injury suffered by consumers as a result of exposure of this information.

THE COURT: Are you serious about that last response?

MR. SCHOSHINSKI: Yes, Your Honor, I am.

THE COURT: So you don't know where the documents came from, you don't know how these people got the possession

of it, you don't know whether they originated from LabMD or some other place, but you are going to use that to show that, because they committed identity theft, that certain individuals were damaged by documents, the source of which you don't even know?

MR. SCHOSHINSKI: Yes, Your Honor.

THE COURT: Holy cow.

So what's the other incident that you are relying on?

MR. SCHOSHINSKI: The other incident is the exposure of the insurance agent file of several thousand consumers.

THE COURT: And when was that?

MR. SCHOSHINSKI: That was in 2008, Your Honor.

THE COURT: And that was through the file-sharing program?

MR. SCHOSHINSKI: That's correct, Your Honor.

THE COURT: And how do you know that they came through the file-sharing program?

MR. SCHOSHINSKI: We know because third parties found the file on file-sharing programs.

THE COURT: Well, I accept that. How do you know that they came through the file-sharing program that was loaded on a computer at LabMD?

MR. SCHOSHINSKI: Based on the evidence we obtained

about the file-sharing program, evidence provided by LabMD that showed that certain files, including this file, were shared on the file-sharing program, we believe that it was exposed through the file-sharing program.

THE COURT: And how many records were shared?

MR. SCHOSHINSKI: Your Honor, I don't have the exact number. I believe it was nine thousand, but I'm not entirely sure.

THE COURT: So are you aware that nine thousand files ended up in some somebody else's hands that were LabMD's files?

MR. RUBINSTEIN: Your Honor, it would be nine thousand individuals. It was one file.

THE COURT: Well --

MR. RUBINSTEIN: And we --

THE COURT: So are you going to dance on the head of a pin now too?

MR. RUBINSTEIN: I'm not dancing on the head of a pin, Your Honor. I appeared before the administrative law judge and --

THE COURT: You can sit down until I'm ready for you.

MR. SCHOSHINSKI: Thank you, Your Honor.

MR. RUBINSTEIN: -- I told him because the FTC said that the files had been shared, our position was then and it

remains to date that the file was taken by this third party, Tiversa.

As you may recall, there was quite a controversy with respect to the government's ability to rely on that file.

THE COURT: It was taken by use of an improperly-loaded file-sharing program.

MR. RUBINSTEIN: It was taken by use of a patented program that Tiversa uses as part of their business model to go from company to company taking files and then coming to the company and saying: Nice business you have here. It would be a shame if anything happened to it. Why don't you hire us to remediate?

In fact, that's what happened here. And part of this was put before --

THE COURT: Was that enabled by the file-sharing program that was loaded by an employee on the computers at LabMD?

MR. RUBINSTEIN: For them to be able to gain access, I don't know.

THE COURT: Why don't you know that?

MR. RUBINSTEIN: Because we don't fully understand the nature and extent of Tiversa's technology.

We attempted to ask them in deposition, and we were met with objections because this is a protected confidential

and highly proprietary piece of software. So we still don't understand to this day.

THE COURT: Well, you can get a protective order in order to access that. Have you asked for that?

MR. RUBINSTEIN: I don't recall. It would be easy enough to check. I can get that for you. I just don't recall whether we did that in the administrative hearing or not. I am certain the question was asked, and I'm certain objections were interposed.

And we had asked -- we actually -- it is very possible that we did, because we filed a motion asking for discovery into the circumstances under which there was a sharing of this information between Tiversa and the FTC.

We discovered that the FTC had worked with Tiversa. In fact, Tiversa gave LabMD's file to another third party.

THE COURT: Well, look, I'm not trying this case, although I am getting a lot of information about the respective positions which also is troubling on both sides.

But I will say --

MR. RUBINSTEIN: The --

THE COURT: So their position, which I guess they are going to present somebody under oath to say that they have traced information through a file-sharing program that allowed some outside source, whether it's Triversa or

somebody else, to wrongfully access information that was on LabMD's computers?

MR. RUBINSTEIN: I don't believe they have done any independent investigation to verify what type of --

THE COURT: I'm not saying that. I'm saying they have got an obligation to present somebody under oath to testify with respect to that, and that's what the deputy director's position -- you are a deputy director; is that right?

MR. SCHOSHINSKI: Your Honor, assistant director.

THE COURT: All right. I would love to promote you if I could, but I can't, so you are still an assistant director.

MR. SCHOSHINSKI: It's the lowest form.

THE COURT: I understand. I know titles are big in agencies. I have been there and played that game for a while.

But the assistant director has just said that there will be evidence presented before a judicial officer, I guess an administrative law judge, in which somebody will state these nine thousand individuals -- information about individuals in a single record was accessed by an outside source through a file-sharing program that had been installed on WebMD's computers.

You are going to say that there is no evidence of

that --

MR. RUBINSTEIN: That's correct.

THE COURT: -- that that ever happened, and you are going to believe that you are right, and the FTC, although sometimes I wonder if they are -- just how compelling their evidence is, that they are going to claim that they are right, and somebody will make a determination of whether there has been a breach or not.

Then the question is -- and I do find this -- and I think I know enough about this, and I learned a lot from the CID hearing -- is that the FTC is going to go into the business of monitoring and investigating and regulating security breaches and that they have decided I think to do that within what they believe is their administrative authority, because I think they went to Congress and Congress wouldn't authorize that for whatever reason, whether it's politics or not.

But I think there has been no amendment to Section 5 to specifically allow that. But they are taking the position that they have the authority to do that.

MR. RUBINSTEIN: That is correct.

THE COURT: I think that there is a significant question about whether Section 5 allows that, but I'm not sure I can decide that based upon my jurisdictional limitations, perhaps.

But I think that's what's going on here is the FTC has staked out a position of regulatory authority and that they are going to advocate that and they are going to advance it to the greatest extent that they can.

You are somebody who is the -- is somebody who has fallen within that ambit of claimed authority, and you claim that you didn't do it. They are going to claim that you did do it.

So there is going to be a factual question of whether or not you did or did not, and then there is going to be a legal question of whether or not they have the authority to do what they have done.

MR. RUBINSTEIN: That's correct. And we are not asking you to decide factual questions today.

THE COURT: I know, but you are asking me to take jurisdiction of this, and I'm not sure I can.

MR. RUBINSTEIN: Well, and I'm happy to do argument with respect to that.

THE COURT: Look, I have spent more time looking at cases than you have on this, so I don't need any more argument on the jurisdictional issue.

MR. RUBINSTEIN: Fair enough.

THE COURT: I mean, I do think it's strange that a judge in New Jersey gets to decide the jurisdictional issue because the posture of the FTC was different in that case

than it is in this case, and then they are arguing that, although I'm co-equal to the judge in New Jersey, that because it came to me a different way, that I can't.

I suspect that they would love to travel forward on the New Jersey decision because it favors them and that they will try to deny the opportunity for another judge to weigh in.

But I think it's a significant -- you ought to find a way, unless you are so hell bent on expanding this jurisdiction or advocating this jurisdiction, to find some way to decide this legal issue.

And I understand why you are doing what you are doing. I have been alive long enough to understand how government and their agencies work. I have been a member of an agency and I understand its impact on defendants or in this case on parties that are under investigation. I understand that too because I have done that as well.

But I think that there is a fundamental jurisdictional legal issue, and there ought to be some way of getting a more definitive ruling than what you have right now.

Because I would hope that you would think that in this current healthcare environment, that the more competition and providers there are for medical detection devices or processes like those offered by LabMD, that the

better off the consuming public is and the better off patients will be. But by your conduct, you have taken one out of the market it looks like.

And if I was an agency head, I would say there has got to be some way of being satisfied that this doesn't happen again, however it happened, and to make sure that we have as many providers as possible out there determining whether or not people do or do not have cancer.

And that that would mean a good faith, transparent, authentic discussion about what your concerns are, and trying to get those allayed by some process which would not be a twenty-year monitoring.

You know, I have defended people that had twenty-year monitoring responsibilities by an agency, big companies, and it's very, very expensive, and it's really intrusive, and in my personal opinion, having been on both sides, they generally are not necessary.

But there is never a middle ground. There should be.

But I would think that it would be in the benefit of all the parties here to say whatever happened, it can't happen again, but whatever you are doing ought to continue to be done, because it benefits the consuming public, which I think is who you are supposed to be protecting under reasonable certainties, that the consuming public would be

treated fairly.

And it's interesting the two people that didn't treat the consuming people fairly are two people in jail that won't even cooperate with you and one of whom you can't even find.

But I don't think that even the FTC thinks that they intentionally wanted this information to get out, because they are subject to HIPAA regulations.

And I will say I have gone into enough doctors' offices and nobody has ever had me sign a statement saying that whatever the obligations are, the rights that I have under the FTC are rights that I have to acknowledge and in some cases give up. It's always HIPAA.

And I think that's what happens when you try to extend into an area where you might be allowed or be permitted to extend, but that assumes, especially on behalf of the government, that they act reasonably.

And here we are, having spent now about an hour and a half, not getting to the fundamental issue here, which I think is how can your interest be accommodated.

And, Mr. Gorji, if you submitted to them a consent order -- and I'm not going to consider that; I don't think it's important -- but it does tell me something about your agency if you say we want twenty years' worth of monitoring and even suggested that was reasonable concerning this

company. No wonder you can't get this resolved, because if that's the opening salvo, even I would be outraged, or at least I wouldn't be very receptive to it if that's the opening bid.

I don't think you believe that this is a company that willy-nilly allows information to be disclosed. I also believe that you don't think, if you remove yourself from the nits and gnats of this dispute, that you would say it was a good idea to make this provider unavailable to patients.

There aren't that many people doing this work as it is. I have another case involving cancer detection processes, and so I know just a little bit about the industry, and one of the regrets of the industry is that there are so few people providing these services. And I think in the current healthcare environment, there will be fewer.

It doesn't serve any of us very well. Some day you are going to need one of those services. I hope it's available.

You have been completely unreasonable about this. And even today you are not willing to accept any responsibility that whatever needs to be done, even if you can't confirm it, that your position is going to be a litigating position, and you will drag four lawyers to a hearing like this.

I mean, I was in a big firm, but on a hearing like this, we wouldn't have four lawyers here. So I don't know what you are trying to accomplish, but I will tell you this, you haven't.

And I have a firm belief that it takes two unreasonable people to create an unreasonable atmosphere that prohibits a reasonable result, and that's where we are.

Your interest is protecting the American public. That's your responsibility.

Your interest is to help a client who I think is providing a good service survive.

And I am confident -- I haven't been in all these depositions. I know this, it's always hard to deal with somebody who is changing lawyers all the time. But to the extent that any of that has irritated you, Mr. Daugherty, you need to settle down. I know you are upset down this, but you are poisoning the atmosphere personally.

And if I was a lawyer representing you, the first thing I would say is you have got to stop the public stuff. If you want to get this resolved and do something well, no government agency is ever going to treat somebody who's advocating publicly and criticizing publicly. They are going to be less accommodating to them. And I have told that to clients over and over and over when I was a lawyer. Now I get to see it from the other end, and now I'm convinced

that's the case.

So to the extent that you have gotten some therapeutic value out of all this, it ought to stop, because your criticism hasn't gotten you to where you want to be, has it? It's gotten you where you don't want to be.

So I understand the legal issues. I thought as I enter my sixties, one of the values I can do is give you some perspective.

Are you a Fiske Scholar? Did you go to the University of Michigan? Did one of you go to Michigan and are a Fiske Scholar?

MR. RUBINSTEIN: I did, Your Honor.

THE COURT: Yeah. Are you a Fiske Scholar?

MR. RUBINSTEIN: Not a Fiske Scholar. I was an Angell Scholar.

THE COURT: All right. Well, never mind. Although I will tell you that the story that if one of you had been that I have is working with Bob Fiske, who I think is one of the finest lawyers in America, that we were once granted jurisdiction, and we always, whenever somebody brought a claim to us to try to request us to expand our jurisdiction, we would have a roundtable discussion to say where within the grant of authority to us is our jurisdiction specifically, and, if not, it needs to go back to the people who are entitled to grant jurisdiction, which we believe was

Congress, and we turn things down.

I think good lawyers -- and he was an agency lawyer for a long time and ran the Southern District for a long time as United States Attorney -- that that lesson has always stuck with me.

So where we are now is I have given you my insights about this. I understand there is no more evidence to be presented.

I don't need any more -- I guess you can cross-examine him if you want. All I hear him saying is that he doesn't like your expert's report and he would have done something differently and he's claimed that HIPAA is what should be, because there are specific standards there -- I think that you will admit that there are no security standards from the FTC. You kind of take them as they come and decide whether somebody's practices were or were not within what's permissible from your eyes.

I too find how does any company in the United States operate when they are trying to focus on what HIPAA requires and to have some other agency parachute in and say, well, I know that's what they require, but we require something different, and some company says, well, tell me exactly what we are supposed to do, and you say, well, all we can say is you are not supposed to do what you did.

And if you want to conform and protect people, you

ought to give them some guidance as to what you do and do not expect, what is or is not required. You are a regulatory agency. I suspect you can do that.

But I think that's what happens when you jump too quickly into something that you want to do, and whether that's circumstances or whether that's agency motivation, I don't know. But it seems to me that it's hard for a company that wants to -- even a company who hires people from the outside and says what do we have to do, and they say you have to do this, but I can't tell you what the FTC rules are because they have never told anybody.

Again, I think the public is served by guiding people beforehand rather than beating them after they -- after-hand. But the assistant director doesn't have the authority to do that. He reports to the deputy director, who reports to the director, who reports to the commission. So he's way down in the pecking order.

So I understand what this witness said.

I suspect that this witness will say that he never consulted with LabMD before about their security processes. He's just come in to opine on the opinions offered by Ms. Hill. Is that correct?

THE WITNESS: Correct.

THE COURT: I kind of wish he had been there before.

One thing I do know is agencies that say you pay for somebody to come in to look at your security practices and this is what an expert said we had to do and needed to do, that they have a different approach, because that's a defense.

But if you want to cross-examine him, now is your time. I had my say.

MR. GORJI: Your Honor, the government has no cross.

THE COURT: So nothing further from Mr. Baker?

We appreciate your testimony.

THE WITNESS: Thank you very much.

THE COURT: You may step down.

Do you have any other witnesses or evidence you want to present?

MR. RAIDER: Not at this time, Your Honor, no.

THE COURT: Anything the FTC wants to present?

MS. FASCETT: Assuming that you are not asking for any argument on the jurisdictional issues, no, nothing further to present. Thank you.

THE COURT: Anything else that LabMD wants to say?

MR. RUBINSTEIN: Your Honor, it's been extensively briefed. If you have any questions, we are glad to answer them. Other than that, we have nothing further.

THE COURT: All right. I will take it under

advisement.

And if there is nothing else to cover today or to present, we will be in recess.

MR. RAIDER: Your Honor, just one quick point before we go to recess?

Was Exhibit 14 admitted into evidence? That's the Monday, January 6th, 2014, letter? If so, we would like to tender it into evidence.

THE COURT: Well, did you tender it?

MR. RAIDER: I thought I did.

THE COURT: Did you object to it?

MR. GORJI: We didn't object, Your Honor.

THE COURT: I guess it's in.

MR. RAIDER: Thank you, Your Honor.

THE COURT: Which is, by the way, what my records reflect was that it was tendered and not objected to and it had been admitted, so you didn't really need to do that. But now it's clear to everybody.

MR. RAIDER: Thank you.

THE COURT: All right. Now we will be in recess.

(Proceedings adjourn at 11:46 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 98 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 7th day of May, 2014.

/s/ Nicholas A. Marrone

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

Exhibit B

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

LabMD, Inc. **Plaintiff,** **v.** **FEDERAL TRADE COMISSION,** **Defendant.**	**1:14-cv-00810-WSD**

OPINION AND ORDER

This matter is before the Court on LabMD's ("Plaintiff") Motion for Preliminary Injunction [2] and the Federal Trade Commission's ("Defendant" or "FTC") Motion to Dismiss the Plaintiff's Complaint [13]. A hearing on the Motion for Preliminary Injunction was conducted on May 7, 2014.

I. BACKGROUND

A. Factual and Procedural History

Plaintiff is a small medical laboratory based in Atlanta, GA, that provided doctors with cancer-detection services. In January, 2010, the Defendant commenced an investigation into the Plaintiff's data security practices regarding

Protected Health Information ("PHI")[1] based upon the claim that sensitive information in the Plaintiff's possession and control had been disclosed by means of a peer-to-peer file sharing network available to the public. Three and a half years later, the Defendant issued an Administrative Complaint against the Plaintiff in which it alleged that there was "reason to believe" that Plaintiff may have engaged in "unfair . . . acts or practices," under 15 U.S.C. § 45(a)(1) of the Federal Trade Commission Act ("Section 5"), because Plaintiff failed to provide reasonably adequate security for patient information retained on its internal network. The Administrative Complaint also alleged that Plaintiff had the capacity to prevent the vulnerabilities in its data security infrastructure "at relatively low cost using readily available security measures," and that the ultimate consumers allegedly harmed due to the Plaintiff's lax data security were unable to protect themselves because they "ha[d] no way of independently knowing" about the alleged disclosures. Def.'s Mot. to Dismiss and Resp. to Pl.'s Mot. for Prelim. Inj. at 7.

The Administrative Complaint cited two specific examples of alleged data

[1] PHI refers to individually identifiable health information, including the individual's name, social security number, address, birth date, history of mental and physical health condition, provision of health care, and payment history for the provision of health care.

security failures at LabMD. First, that LabMD failed to discover that its billing manager had installed a peer-to-peer file sharing application known as Limewire on his or her work computer, and a file that contained personal information on approximately 9,300 consumers was accessible to any individual, who used or had access to Limewire's software. Second, that the police department in Sacramento, California arrested alleged identity thieves, and found, in their possession, LabMD's documents containing sensitive pertinent personal information on individuals.[2]

On November 12, 2013, Plaintiff moved the Commission to dismiss the Administrative Complaint on the grounds that the FTC had no statutory authority to address the data security practices of private companies under Section 5, and that the application of Section 5 to LabMD's data security practices violated the Due Process Clause of the United States Constitution. On January 16, 2014, the Commission denied the Plaintiff's Motion to Dismiss, concluding that Section 5 vests the FTC with authority to address a private company's data security practices "as unfair . . . acts or practices" if they are found to be so deficient that it "causes

[2] At the May 7, 2014, Preliminary Injunction hearing, the FTC informed the Court that it was unaware whether the alleged identity thieves arrested in Sacramento received documents containing PHI as a consequence of LabMD's data security failures.

or is likely to cause substantial injury to consumers [that] is not reasonably avoidable by consumers themselves and [the harm is] not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n). The Commission also found that the Administrative Complaint sufficiently stated a claim that the Plaintiff engaged in "unfair . . . acts or practices" because of its alleged failure to maintain adequate data security, and stressed that the "ultimate decision on LabMD's liability will depend on the factual evidence to be adduced in this administrative proceeding." Pl.'s Ex. 3 at 18.

The claims alleged in the Administrative Complaint have been referred to an administrative law judge ("ALJ") in the underlying adjudicatory proceeding. On May 20, 2014, the ALJ will conduct an evidentiary hearing to determine whether the Plaintiff's data security practices violated Section 5. After the ALJ issues an initial decision, either party may appeal to the Commission for *de novo* review of the ALJ's factual findings and legal conclusions. 5 U.S.C. § 557(b). If the Commission concludes that the Plaintiff engaged in "unfair . . . acts or practices," and enters a cease and desist order, the Plaintiff has a statutory right to "obtain a review of such order in the court of appeals." 15 U.S.C. § 45(c).

On November 14, 2013, the Plaintiff filed a complaint against the FTC in the United States District Court for the District of Columbia, seeking to enjoin the

enforcement action on the grounds that (1) the FTC abused its statutory authority by regulating LabMD's data security practices, (2) the FTC's application of Section 5 to LabMD's data security practices violated the Due Process Clause, and (3) the FTC brought the enforcement action to retaliate against LabMd's President's public criticism of the agency. On December 23, 2013, the Plaintiff filed in the Eleventh Circuit a Motion to Stay the administrative proceedings, arguing that a stay was necessary to prevent irreparable harm, including on the grounds that the FTC's application of Section 5 to LabMD's data security practices lacked statutory authority, and the FTC's actions were *ultra vires* and unconstitutional. On February 18, 2014, the Eleventh Circuit, *sua sponte*, dismissed the Plaintiff's petition for lack of jurisdiction.

The Eleventh Circuit concluded that its authority, under § 45(c), did not extend beyond review of a final cease and desist order. The Eleventh Circuit, however, "[did] not express or imply any opinion about whether a district court has jurisdiction to hear [the plaintiff's] claims or about the merits of those claims."

On February 19, 2014, the Plaintiff voluntarily dismissed its complaint pending before the United States District Court for the District of Columbia. A month later, the Plaintiff filed a Verified Complaint ("Complaint") for Declaratory and Injunctive relief in this Court. The Complaint alleges that (1) the FTC action

is arbitrary and capricious under the Administrative Procedures Act ("APA") because the FTC does not have the statutory authority to regulate PHI under Section 5; (2) the FTC action is an *ultra vires* act that exceeds its congressional and constitutional authority; and (3) the FTC's application of Section 5 to LabMD's data security practices violates the requirements of fair notice, and the right to a fair hearing in a fair tribunal under the Due Process Clause of the United States Constitution. The Complaint also alleges that the FTC violated LabMD's First Amendment right to free speech by filing the Administrative Complaint. On March 20, 2014, Plaintiff filed a Motion for Preliminary Injunction to enjoin the ongoing administrative proceeding before the ALJ, and to enjoin the FTC from asserting any further data security actions against LabMD.

At the core, LabMD's claims in this matter are identical to those filed in the United States District Court for the District of Columbia and the Eleventh Circuit. LabMD alleges that Section 5 does not authorize an action for alleged security breaches involving PHI that is not provided to LabMD by patients but by physicians ordering laboratory tests for their patients. It claims also that PHI is regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPPA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, which discredits that the FTC has the authority to

regulate data security under Section 5. LabMD further alleges that the FTC has not published any requirements for the protection of patient information, and thus LabMD is not on notice of what protections the FTC now claims were required. LabMD claims that the FTC brought its enforcement action against LabMD to retaliate against its President's public criticism of the FTC, which were published through the press, social media, and in a book entitled The Devil Inside the Beltway: The Shocking Expose of the US Government's Surveillance and Overreach into Cybersecurity, Medicine and Small Business.[3]

On April 7, 2014, the FTC replied to LabMD's Motion for Preliminary Injunction, and moved under Rule 12(b)(1) of the Federal Rules of Civil Procedure to dismiss the Complaint for lack of jurisdiction and moved under Rule 12(b)(6) to dismiss for failure to state a claim. On April 11, 2014, LabMD filed its Response in Opposition to the FTC's Motion to Dismiss. On April 16, 2014, the FTC replied to LabMD's Response to its Motion to Dismiss the Complaint.

[3] At the May 7, 2014 hearing, Mr. Daugherty testified that FTC employees accessed his blog 75 times shortly after he criticized the FTC for bringing an enforcement action against LabMD. Preliminary Injunction Hr'g Tr., May 7, 2014, at 23: 9-20. Counsel for the FTC did not know why FTC personnel repeatedly accessed Mr. Daugherty's blog shortly after the criticisms were published, but surmised that a possible explanation for accessing the blog was that FTC personnel wanted to ensure that Mr. Daugherty's free speech rights were not impeded. Id. at 24-28.

II. DISCUSSION

A. Legal Standard

1. Motion to Dismiss

The law governing motions to dismiss pursuant to Rule 12(b)(6) is well-settled. Dismissal of a complaint is appropriate "when, on the basis of a dispositive issue of law, no construction of the factual allegations will support the cause of action." Marshall Cnty. Bd. of Educ. v. Marshall Cnty. Gas Dist., 992 F.2d 1171, 1174 (11th Cir. 1993).

In considering a motion to dismiss, the Court accepts the plaintiff's allegations as true and considers the allegations in the complaint in the light most favorable to the plaintiff. See Hishon v. King & Spalding, 467 U.S. 69, 73 (1984); Watts v. Fla. Int'l Univ., 495 F.3d 1289, 1295 (11th Cir. 2007); see also Bryant v. Avado Brands, Inc., 187 F.3d 1271, 1273 n.1 (11th Cir. 1999) ("At the motion to dismiss stage, all well-pleaded facts are accepted as true, and the reasonable inferences therefrom are construed in the light most favorable to the plaintiff."). The Court, however, is not required to accept a plaintiff's legal conclusions. See Sinaltrainal v. Coca-Cola Co., 578 F.3d 1252, 1260 (11th Cir. 2009) (citing Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009)), abrogated on other grounds by Mohamad v. Palestinian Auth., 132 S. Ct. 1702 (2012). The Court also will not

"accept as true a legal conclusion couched as a factual allegation." See Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007). Ultimately, the complaint is required to contain "enough facts to state a claim to relief that is plausible on its face." Twombly, 550 U.S. at 570.[4]

To state a claim to relief that is plausible, the plaintiff must plead factual content that "allows the Court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Iqbal, 556 U.S. at 678. "Plausibility" requires more than a "sheer possibility that a defendant has acted unlawfully," and a complaint that alleges facts that are "merely consistent with" liability "stops short of the line between possibility and plausibility of 'entitlement to relief.'" Id. (citing Twombly, 550 U.S. at 557). "To survive a motion to dismiss, plaintiffs must do more than merely state legal conclusions; they are required to allege some specific factual bases for those conclusions or face dismissal of their claims." Jackson v. BellSouth Telecomms., 372 F.3d 1250, 1263 (11th Cir. 2004) ("[C]onclusory allegations, unwarranted deductions of facts or legal conclusions

[4] The Supreme Court explicitly rejected its earlier formulation for the Rule 12(b)(6) pleading standard: "'[T]he accepted rule [is] that a complaint should not be dismissed for failure to state a claim unless it appears beyond doubt that the plaintiff can prove no set of facts in support of his claim which would entitle him to relief.'" Twombly, 550 U.S. at 577 (quoting Conley v. Gibson, 355 U.S. 41, 45-46 (1957)). The Court decided that "this famous observation has earned its retirement." Id. at 563.

masquerading as facts will not prevent dismissal.") (citations omitted).[5]

B. Analysis

Under § 704 of the APA, "[a]gency action made reviewable by statute and final agency action for which there is no other adequate remedy in a court are subject to judicial review." 5 U.S.C. § 704. "The requirement of a final agency action has been considered jurisdictional. If the agency action is not final, the court therefore cannot reach the merits of the dispute." Nat'l Parks Conservation Ass'n v. Norton, 324 F.3d 1229, 1236 (11th Cir. 2003) (internal citations and quotation marks omitted). An agency action is considered final when two requirements are met: (1) the action marks the "consummation of the agency's decisionmaking process"—it must not be of a tentative or interlocutory nature, and (2) the action must be one by which "rights or obligations have been determined" or from which "legal consequences will flow." Bennett v. Spear, 520 U.S. 154, 177-78 (1994). A non-final agency action is one that "does not itself adversely affect the complainant but only affects his rights adversely on the contingency of

[5] Federal Rule of Civil Procedure 8(a)(2) requires the plaintiff to state "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). In Twombly, the Supreme Court recognized the liberal minimal standards imposed by Federal Rule 8(a)(2) but also acknowledged that "[f]actual allegations must be enough to raise a right to relief above the speculative level . . . ." Twombly, 550 U.S. at 555.

future administrative action." Rochester Tel. Corp. v. United States, 307 U.S. 125, 130 (1939).

LabMD contends that the Commission's interlocutory decision to deny its Motion to Dismiss the Administrative Complaint is a final agency action because the Commission has concluded that Section 5 allows the FTC to regulate PHI retained by medical service providers, and, that the FTC is authorized to impose obligations on those providers who maintain PHI even if it supplements the requirements of other federal statutes. LabMD also argues that the FTC has treated the Commission's Order as a final agency action because the FTC submitted the Order to the Eleventh Circuit and the District Court of New Jersey as supplemental legal authority, requesting those courts to afford Chevron deference to the Commission's interpretation of Section 5.

While the Eleventh Circuit has not directly addressed the issue, those courts that have universally hold that a direct attack on the agency's statutory or constitutional authority to conduct an investigation or commence an enforcement action does not allow a plaintiff to evade administrative review or avoid administrative procedures. Aluminum Co. of America v. United States, 790 F.2d 938, 942 (D.C. Cir. 1986) (observing that a claim attacking an agency's assertion of jurisdiction as beyond statutory authority does not make a difference to the

finality analysis because the purpose of finality is to prevent piecemeal "consideration of rulings that may fade into insignificance by the time the initial decisionmaker disassociates itself from the matter."); see also VeldHoen v. United States Coast Guard, T.A., 35 F.3d 222 (5th Cir. 1994); Dairymen, Inc. v. FTC, 684 F.2d 376, 378-79 (6th Cir. 1982).

The Commission's denial of LabMD's Motion to Dismiss the Administrative Complaint on the grounds that the FTC does not have the statutory authority to regulate data security practices under Section 5 is the type of Order that "ha[s] long been considered nonfinal." DRG Funding Corp. v. Secretary of HUD, 76 F.3d 1212, 1215 (D.C. Cir. 1996). The Commission's Order is the equivalent of a district court's decision to deny a motion to dismiss, "which—unlike a final order ending the case—assures its continuation." Id. LabMD's contention that the Commission's interlocutory Order is a final agency action because it concluded that the FTC has statutory authority to regulate PHI under Section 5 has specifically been rejected by other courts.

In American Airlines Inc. v. Herman, for example, the plaintiff argued that it would be "futile for it to pursue the administrative process because the DOL already has finally and definitively rejected each of [the] challenges to its statutory and regulatory authority." 176 F.3d 283, 292 (5th Cir. 1999). The Fifth Circuit

rejected the plaintiff's argument, and held that "the requirement that the reviewable order be definitive in its impact on the rights of the parties is something more than a requirement that the order be unambiguous in legal effect. It is a requirement that the order have some substantial effect *which cannot be altered by subsequent administrative action*." Id. (internal quotation marks and citations omitted) (emphasis in original). Because of the possibility that the plaintiff could prevail on the merits in the administrative proceeding, the Fifth Circuit required the plaintiff to submit to the administrative proceeding. Id.

The Court concludes that it does not have jurisdiction over this action because even if it determines that the Commission's position on the FTC's authority to regulate PHI under Section 5 was definitive, the mere assertion of jurisdiction does not impose or fix an obligation on LabMD from which "legal consequences may flow." Bennett, 520 U.S. at 177-78. The Commission's denial of LabMD's Motion to Dismiss the Administrative Complaint is not a final agency action, and the FTC's decision to submit the Commission's Order to other courts as "supplemental authority" is a litigation tactic that does not render final a Commission Order that is not. The possibility that LabMD may prevail on the merits if the ALJ, or the Commission, concludes that it did not violate Section 5 will moot its judicial challenge and render it unnecessary for the Court to intervene

in an ongoing administrative proceeding.[6] American Airlines Inc., 176 F.3d at 292. See also FTC v. Standard Oil Co. of California, 449 U.S. 232, 242 (1980) (observing that "judicial intervention into the agency process denies the agency an opportunity to correct its own mistakes and to apply its expertise," and that "intervention also leads to piecemeal review which at the least is inefficient and upon completion of the agency process might prove to have been unnecessary.") (citations omitted).

LabMD alleges that the burdens imposed by the FTC investigation and the requirement to submit to an administrative proceeding crippled its day to day business because it had to effectively shut down its operations, lay off more than two dozen employees, and cannot procure medical malpractice and property insurance to remain a going concern. Even if the Court accepts these allegations as true, the expense and burdens associated with complying with an agency's information requests and submitting to an administrative proceeding do not qualify as legally recognized harms, and do not provide a basis upon which to grant

[6] The Court believes that the likelihood of a favorable jurisdictional or merits outcome for LabMD is slight, but that belief cannot govern the legal issues addressed in this Order. As the Court noted at the May 7, 2014 hearing, the authority of the FTC to enlarge its regulatory activity in the data security area presents an interesting and likely important jurisdictional issue that needs to be resolved promptly.

LabMD relief. Standard Oil Co. of California, 449 U.S. at 244 ("litigation expense, even substantial and unrecoupable cost, does not constitute irreparable injury" because "the expense and annoyance of litigation is part of the social burden of living under government.") (internal citations and quotation marks omitted); see also Imperial Carpet Mills, Inc. v. Consumer Prod. Safety Comm'n, 634 F.2d 871, 874 (5th Cir. Unit B Jan. 1981)[7] (holding that "the burden of defending against the Complaint; the expense of complying with the Commission's anticipated final order; the resulting bad publicity; and the potential for a dangerous loss of credit" do not justify intervention into administrative agency action).[8]

[7] In Bonner v. City of Prichard, the Eleventh Circuit adopted as binding precedent decisions of the Fifth Circuit handed down prior to October 1, 1981. 661 F.2d 1206, 1209-10 (11th Cir. 1981).

[8] LabMD's claim that the FTC investigation had a crippling effect on its business is questionable in light of Mr. Daugherty's testimony at the Preliminary Injunction hearing. In 2010, the FTC began its investigation into LabMD's data security practices. Four years later, in January, 2014, LabMD decided to no longer provide cancer detection services, which is the essence of its business operations. Preliminary Injunction Hr'g Tr., at 6: 20-25. LabMD continued to operate as a going concern throughout the FTC investigation until the end of 2013. In 2013, LabMD retained 25 to 30 employees on its payroll, and it continued to generate a profit margin of approximately 25% until 2013 when the company experienced a loss of half a million dollars. Id. at 11: 1-25. The company "never had problems getting insurance prior to 2013." Id. at 12: 6-8. The evidence presented at the Preliminary Injunction hearing demonstrates that an insurer's decision to deny tail risk coverage to LabMD on account of the FTC investigation and administrative

LabMD's view that the Court can address and review its constitutional claims based on the Due Process Clause and the First Amendment regardless of whether there is a final agency action under the APA is contrary to established precedent. In Ticor Tile Ins. Co. v. FTC, the plaintiff mounted a facial challenge to the constitutionality of Section 5, arguing that the FTC had definitively concluded that the provision was constitutional, and that the FTC's position constituted final agency action reviewable in a federal court before the consummation of the administrative proceeding. 814 F.2d 731, 738-743, 746-749 (D.C. Cir. 1987). The D.C. Circuit affirmed the dismissal of plaintiff's complaint because there was no final agency action, the plaintiff did not exhaust its remedies in the administrative proceeding, and the case was not ripe for review. Id. at 732; Id. at 748 (Williams, J.) (explaining that even if unconstitutional actions are accepted as "heavier" than "those of statutory illegality, the constitutional dimension of appellants' burden entails a concern that militates powerfully against

---

proceeding was not made until January 13, 2014, which is a week after LabMD had decided to discontinue its cancer detection services. See Pl.'s Ex. 15, attached to Pl.'s Ex. List. At the Preliminary Injunction hearing, Mr. Daugherty, conceded that the implementation of the Affordable Care Act, and its resulting effect on cost containment and market consolidation negatively impacted LabMD's operations, and "creat[ed] huge anxiety, destruction, consolidation in our customer base." Id. at 52: 9-21. Mr. Daugherty also conceded that LabMD's future "depend[ed] on Obamacare, and other than that I don't know." Id. at 54: 1-4.

immediate review: the fundamental rule of judicial restraint, forbidding resolution of constitutional questions before it is necessary to decide them.") (internal citations and quotation marks omitted).

In the absence of final agency action, LabMD's alleged constitutional injuries are not currently ripe for review. North Carolina State Bd. of Dental Examiners v. FTC, 768 F. Supp. 2d 818, 824 (E.D.N.C 2011) (holding that in the absence of a final cease and desist order from the Commission, plaintiff has failed to show that its constitutional rights have been or are being violated); see also E. I. Dupont de Nemours and Co. v. FTC, 488 F. Supp. 747, 754 (D. Del. 1980) (rejecting the plaintiff's claim that the FTC violated its First Amendment rights by filing a complaint because the FTC did not direct the plaintiff to stop engaging in speech, and there was no indication that significant costs or sanctions on the use of protected expression would be imposed on the plaintiff to stifle its free speech as the "only 'threat' that is involved in the administrative proceedings is the threat that a cease and desist order will be issued [and] . . . no other sanctions or penalties can be imposed . . . as the result of those proceedings.").

Finally, LabMD asserts that even if the Commission's Order regarding its jurisdiction does not constitute final agency action, the Leedom exception applies, allowing the Court to review LabMD's constitutional and *ultra vires* claims.

Under the Leedom exception, federal courts typically lack jurisdiction to enjoin an ongoing administrative proceeding, Ewing v. Mytinger & Casselberry, Inc., 339 U.S. 594, 598 (1950), unless the agency commits an "egregious error" that plainly violates an unambiguous and mandatory provision of a federal statute, and the aggrieved party has no adequate or meaningful opportunity to vindicate its rights. Leedom v. Kyne, 358 U.S. 184 (1958); American Airlines Inc., 176 F.3d at 293-94. The Court concludes that the Leedom exception does not apply here because the FTC's application of Section 5 to the data security practices of private companies is not contrary to an unambiguous and mandatory provision of a federal statute. In American Airlines Inc., the Fifth Circuit specifically held that the Leedom exception does not apply to a "dispute over whether an agency charged with a statute's implementation has interpreted it correctly." 176 F.3d at 293. That is the crux of the Plaintiff's Complaint in this matter, but it is insufficient to invoke the exception under Leedom. LabMD can obtain meaningful and adequate review of its jurisdictional challenge in the Court of Appeals, if that is necessary.

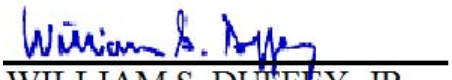
III. CONCLUSION

Accordingly, for the foregoing reasons,

IT IS HEREBY ORDERED that the Defendant's Motion to Dismiss the Complaint for lack of jurisdiction is **GRANTED** [13].

IT IS FURTHER ORDERED that the Plaintiff's Motion for Preliminary Injunction is **DENIED AS MOOT** [2].

SO ORDERED this 12th day of May 2014.



WILLIAM S. DUFFEY, JR.
UNITED STATES DISTRICT JUDGE

Exhibit C

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

LabMD, Inc., Plaintiff, vs. Federal Trade Commission, Defendant.	CIVIL ACTION FILE NO. 1:14-cv-810-WSD

J U D G M E N T

This action having come before the court, Honorable William S. Duffey, Jr., United States District Judge, for consideration of Defendant's Motion to Dismiss, and the court having granted said motion, it is

Ordered and Adjudged that the action be, and the same hereby, is **dismissed**.

Dated at Atlanta, Georgia, this 12th day of May, 2014.

JAMES N. HATTEN
CLERK OF COURT

By: s/ Ashley Coleman
Deputy Clerk

Prepared, Filed, and Entered
in the Clerk's Office
May 13, 2014
James N. Hatten
Clerk of Court

By: s/ A. Coleman
Deputy Clerk

Exhibit D

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

LabMD, INC., Plaintiff, v. FEDERAL TRADE COMMISSION, Defendant.	)	Civil Action No.: _____ *Related Case*: FTC v. LabMD et al., 1:12-cv-3005-WSD

VERIFIED COMPLAINT
FOR DECLARATORY AND INJUNCTIVE RELIEF

Plaintiff LabMD, INC. ("LabMD") hereby states its complaint for declaratory and injunctive relief against the unconstitutional abuse of government power and ultra vires actions by Defendant Federal Trade Commission (the "FTC" or "Commission") as follows:

PARTIES, JURISDICTION, AND VENUE

1. LabMD, 1250 Parkwood Circle, Unit 2201, Atlanta, GA 30339, is a small medical cancer diagnostics business.

2. The FTC, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580, is a federal agency for purposes of the Administrative Procedure Act ("APA"), 5 U.S.C. § 551 et seq.

3. This Court has subject-matter jurisdiction under 28 U.S.C. § 1331, 28 U.S.C. § 2201, and 5 U.S.C. § 702. In LabMD v. FTC, Case No. 13-15267-F, at 2 (11th Cir. Feb. 18, 2014), the United States Court of Appeals for the Eleventh Circuit examined whether it had jurisdiction to entertain LabMD's claims against the FTC under the APA, as codified in relevant part at 5 U.S.C. §§ 701-06, under the federal Constitution, and under 28 U.S.C. § 1331, which allows for "nonstatutory" review of ultra vires agency actions. The Court held:

> [J]urisdiction to hear suits under the APA is conferred by 28 U.S.C. § 1331, which provides district courts original jurisdiction of all civil actions arising under the laws of the United States. Any APA, *ultra vires*, and constitutional claims, to the extent they can be asserted [by LabMD] at this stage, first must be asserted and considered in a district court.

(internal citations omitted). A true and correct copy of the foregoing Order is attached hereto as Exhibit 1 and is incorporated herein by reference. See also Sackett v. E.P.A., 132 S. Ct. 1367, 1373 (2012) (". . . the APA provides for judicial review of all *final* agency actions . . . ."); id. at 1374 ("The Court holds that the Sacketts may immediately litigate their jurisdictional challenge in federal court. I agree, for the Agency has ruled definitively on that question.") (Ginsburg, J. concurring). The grounds for the relief requested include the due process clause of the United States Constitution, 5 U.S.C. §§ 701-706 (APA's judicial review provisions), 28 U.S.C. §

1651 (the All Writs Act), 28 U.S.C. § 2201 (the Declaratory Judgment Act), and 28 U.S.C. § 2202 (further relief).

4. The FTC has finally determined that it has jurisdiction over LabMD and that it has complied with constitutional due process fair-notice requirements: In the Matter of LabMD, Inc., FTC Dkt. No. 9357 (Jan. 16, 2014). A true and correct copy of the foregoing order is attached hereto as Exhibit 2 and is incorporated herein by reference.

5. The FTC claims the foregoing decision marks the consummation of its decisionmaking process, has the force of law, and is entitled to deference under "Chevron." See Supplemental Letter Brief, FTC v. Wyndham Worldwide Corp. et al., Case No. 2:13-cv-01887-ES-JAD, Dkt. 152-1, at 6 (Jan. 21, 2014). A true and correct copy of the foregoing brief is attached hereto as Exhibit 3 and is incorporated herein by reference.

6. Venue is proper under 28 U.S.C. §1391(e).

NATURE OF THE CASE

7. LabMD, at all relevant times a small medical laboratory providing doctors with cancer-detection services, is now on the verge of ceasing all operations after being trapped in a paralyzing web of government investigations, subpoenas, and administrative litigation.

8. At some unknown point between 2005 and August 2013, the FTC, through enforcement activities and/or internet postings on the FTC's website, rather than through administrative rulemaking, guidance or known standards, declared for the first time that certain unspecified patient-information data-security practices employed by LabMD were inadequate and thus an "unfair" trade practice under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("Section 5").

9. The FTC still has yet to issue any rule or statement with legal force and effect describing the specific patient-information data-security practices it believes Section 5 prohibits or permits.

10. Between 2005 and the present, the FTC never specified in a rule or statement with legal force and effect how LabMD's patient-information practices fell short or described what, exactly, it should have done differently at any given point. In fact, the FTC commenced an investigation of LabMD in January 2010, filed its administrative complaint in August 2013, and still today, LabMD has yet to be told what, exactly, it did wrong at any point during the relevant period of years.

11. The FTC's actions and a campaign of disparagement, including conclusory statements by an FTC Commissioner that LabMD had mishandled sensitive patient information made shortly after the administrative complaint had been filed, have eviscerated LabMD's business and destroyed its professional reputation.

12. In October, 2013, LabMD lost its directors and officers (D&O) liability insurance as a result of the pending enforcement action and has been unable to obtain D&O insurance because of the pending action.

13. Further, LabMD and its doctors were denied "tail" medical malpractice insurance because of the FTC's actions, which will, unless this matter is resolved favorably in the near future, severely limit LabMD's prospects for obtaining medical malpractice insurance going forward and thus hiring qualified physicians.

14. The company's insurance carrier has advised that it will not renew LabMD's general liability insurance policy effective May 6, 2014, so that the policy will terminate effective October, 2014. This means that LabMD cannot rent office space.

15. The FTC's actions have forced LabMD, a company that once employed more than forty people and provided diagnostic services to more than one hundred doctors, to stop accepting samples.

16. At all times relevant, LabMD's Protected Health Information ("PHI"), or patient-information, data-security practices were subject to comprehensive regulation by the U.S. Department of Health and Human Services ("HHS") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 U.S.C. § 1320d et seq., and the Health Information Technology for Economic and Clinical Health Act

("HITECH"), 42 U.S.C. §§ 300jj et seq., 17901 et seq. See http://www.healthit.gov/providers-professionals/ehr-privacy-security/practice-integration .

17. Neither the HHS nor the FTC has accused LabMD of violating HIPAA or HITECH. See Complaint, In the Matter of LabMD, Inc., FTC Dkt. No. 9357 (Aug. 28, 2013). A true and correct copy of the foregoing complaint is attached hereto as Exhibit 4.

18. Even if Section 5 does empower the FTC to broadly regulate data-security, which it does not, Congress delegated sole authority to regulate PHI data-security to the HHS. And even if Section 5 does empower the FTC to regulate PHI data-security concurrently with HHS and/or to "overfile" HHS using a "common law" of consent orders and internet posts to impose requirements in excess of those set through HHS rulemaking, which it does not, the Commission's refusal to promulgate rules or regulations and provide the public with proper notice and comment violates LabMD's due process rights by failing to give fair notice of what the FTC believes Section 5 forbids or requires.

19. Not only does the FTC lack the statutory authority to regulate PHI and/or cyber-security, it also lacks the expertise to do so. For example, Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," 78 Fed. Reg. 11739 (Feb.

19, 2013), available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (accessed Mar. 18, 2014), directed the Department of Commerce to set data-security standards, not the FTC.

20. To stop the abuse, LabMD seeks a declaration that the FTC lacks jurisdiction under Section 5 over PHI data-security practices and that the FTC has violated LabMD's due process and First Amendment rights. It also seeks preliminary and permanent injunctive relief staying the administrative proceedings in In the Matter of LabMD, Inc., FTC Dkt. No. 9357. Finally, LabMD asks that the FTC pay all of LabMD's attorneys' fees and litigation costs.

FACTS

21. Section 5 authorizes the FTC to prohibit "unfair or deceptive acts or practices in or affecting commerce."

22. The FTC in this case claims Section 5 "unfairness" authority to regulate LabMD's PHI data-security practices, even absent a claim of "deception," by way of administrative "common law" established through consent orders and Internet postings.

I. The FTC Targets LabMD.

23. In or about 2008, Tiversa Holding Corp. ("Tiversa"), a self-described "cyber-intelligence company" specializing in searching for and copying medical,

financial, and other sensitive files on peer-to-peer networks using patented technology, obtained a LabMD accounts-receivable computer file containing PHI without LabMD's knowledge or consent.

24. On May 13, 2008, Tiversa contacted LabMD, advised it that Tiversa had taken its property, and refused to provide information on the procurement of the file unless LabMD entered into a contract for Internet security services. LabMD turned down this offer. See Dissenting Statement of Commissioner J. Thomas Rosch, Petitions of LabMD, Inc. and Michael J. Daugherty to Limit or Quash the Civil Investigative Demands, FTC File No. 1023099 (June 21, 2012). A true and correct copy of the foregoing dissent is attached hereto as Exhibit 5 and is incorporated herein by reference.

25. In 2009, Tiversa gave LabMD's PHI accounts-receivable file to the FTC under highly irregular circumstances. See id. Recent deposition testimony of Tiversa's CEO, Robert Boback, suggests the FTC and Tiversa met on multiple occasions and ultimately conspired and agreed to transfer LabMD's file via a FTC civil investigative demand (CID) to a third company (the "Privacy Institute") that, upon information and belief, is a company that has a relationship with a Tiversa advisory board member.

26. Beginning in January 2010, the FTC requested and LabMD voluntarily provided thousands of pages of documents and submitted to multiple meetings and interviews.

27. Then, on December 21, 2011, the FTC issued formal civil investigative demands (the "CIDs") to LabMD.

28. LabMD filed a Petition to Limit or Quash the CIDs on January 10, 2012, explaining, among other things, that LabMD's PHI data security was exclusively regulated by HHS and solely subject to HHS rules and regulations establishing data-security standards for PHI under HIPAA and HITECH.

29. Commissioner Julie Brill denied LabMD's petition on April 20, 2012. Commission Letter Denying LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand and Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand, in File No. 1023099, at 13 (April 20, 2012). A true and correct copy of the foregoing correspondence is attached hereto as Exhibit 6 and is incorporated herein by reference.

30. Commissioner Brill acknowledged that LabMD's PHI accounts-receivable spreadsheet file "can be considered" protected health information regulated under HIPAA and HITECH but claimed that the FTC jurisdiction under Section 5 was "overlapping and concurrent." Id.

31. On April 25, 2012, LabMD appealed Commissioner Brill's ruling, arguing, as the Commission recently admitted, that the FTC "does not enforce HIPAA or HITECH." See Ex. 2 at 12 & n.19. LabMD also challenged the FTC's reliance on the PHI accounts-receivable file obtained from Tiversa.

32. Nonetheless, on June 21, 2012, three Commissioners (including Commissioner Brill) affirmed Commission Brill's ruling, "finding its conclusions to be valid and correct." See Commission Letter Affirming the Ruling, By Commissioner Brill, Denying the Petitions To Limit or Quash Filed by LabMD and Michael J. Daugherty (June 21, 2012). A true and correct copy of the foregoing order is attached hereto as Exhibit 7 and is incorporated herein by reference. Then-Commissioner Thomas Rosch dissented. Ex. 5.

33. The FTC then filed a petition to enforce the CIDs in this Court. LabMD opposed the petition, arguing, among other things, that the FTC lacked jurisdiction to regulate data-security.

34. The Hon. William S. Duffey upheld the CIDs, but said "there is significant merit" to LabMD's argument that Section 5 does not justify an investigation into data-security practices and consumer privacy issues. See Opinion and Order, FTC v. LabMD et al., 1:12-cv-3005-WSD, Dkt. No. 23, at 4 (N.D. Ga.

Nov. 26, 2012) (Duffy, J.). A true and correct copy of the foregoing order is attached hereto as Exhibit 8.

II. LabMD Publicly Criticizes The FTC And The FTC Retaliates.

35. LabMD's owner, Michael Daugherty decided to warn the public about the FTC's abuses through the press, social media, and a book. Mr. Daugherty used, and continues to use, his website, http://michaeljdaugherty.com/, to criticize the government.

36. For example, Mr. Daugherty was quoted in a September 7, 2012, Atlanta Business Chronicle article as follows: "'We are guilty until proven innocent with these people . . . . They are on a fishing expedition. We feel like they are beating up on small business.'" Amy Wenk, "Atlanta Medical Lab Facing Off Against FTC," Atlanta Business Chronicle (September 5, 2012). Ms. Wenk wrote that "Daugherty contends his company is being unreasonably persecuted by FTC. He said he's already spent about $500,000 fighting the investigation." Id.

37. On information and belief, FTC attorney Alain Sheer, who would later serve as lead counsel for the FTC in an enforcement action against Plaintiff, monitored Mr. Daugherty's political speech and retaliated against him for it.

38. For example, on July 19, 2013, Mr. Daugherty posted the trailer to his book, "The Devil Inside the Beltway," on his website,

http://michaeljdaugherty.com/2013/07/19/the-devil-inside-the-beltway-book-trailer/. The trailer called the FTC's actions against LabMD an "abusive government shakedown" and explained that his book would "blow the whistle" about how "the Federal Trade Commission began overwhelming . . . [LabMD, a] small business, a cancer detection center, with their abusive beltway tactics." It criticized Commission staff, including Mr. Sheer.

39. On July 22, 2013, Mr. Sheer told LabMD that Commission staff had recommended that the FTC commence enforcement proceedings against LabMD.

40. On July 30, 2013, Janis Claire Kestenbaum, the Senior Legal Advisor to the Chairwoman of the FTC, provided LabMD a draft complaint.

41. On August 28, 2013, the Commission commenced an enforcement action (the "Enforcement Action") by issuing a complaint and notice order. The gravamen of its claim at that time was about the PHI accounts-receivable file purloined by Tiversa. Mr. Sheer, who met with Tiversa and who was responsible for the shell-game through which the FTC obtained the file, is lead Complaint Counsel.

42. The FTC's Complaint in the Enforcement Action makes clear that LabMD was a "health care provider" and subject to HIPAA, which comprehensively regulates patient-information data-security, among other things.

43. The FTC did not allege that LabMD violated PHI data-security standards and breach-notification requirements established by HIPAA and HITECH and HHS regulations implementing those statutes.

44. Instead, the FTC's Complaint solely alleged that LabMD violated Section 5's proscription against "unfair" trade practices. It said LabMD's "information security program" was not "comprehensive" and that LabMD did not use "readily available measures" or "adequate measures" but did not specify what those terms actually mean. See Ex. 4 ¶¶ 10-11.

45. The FTC did not name an individual complainant or allege direct harm to any person.

46. The FTC did not cite any regulations, guidance, or standards for what was "adequate," "readily available," "reasonably foreseeable," "commonly known," or "relatively low cost."

47. The FTC did not cite any regulations, guidance, or standards that LabMD supposedly failed to comply with, or specify the combination of LabMD's alleged failures to meet the unspecified regulations, guidance, or standards that, "taken together," allegedly violated Section 5.

48. The FTC did not allege that LabMD's data-security practices fell short of meeting medical-industry data-security standards, such as those established by HIPAA and HITECH for PHI data security.

49. Mr. Sheer of the FTC has admitted that "[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward." Initial Pretrial Conference Transcript, In the Matter of LabMD, Inc., Dkt. No. 9357, 10:11-15 (Sept. 25, 2013) ("Initial Pretrial Conf. Trans."). He also acknowledged that the FTC brought this action without any complaining witnesses who say their data was released or disclosed. Id. 33:3-5. A true and correct copy of that transcript is attached hereto as Exhibit 9.

50. No court has ever held the FTC may require firms to adopt information-practice policies under Section 5's "unfairness" prong. Hearing Trans. 16: 22-25, FTC v. LabMD, Inc. et al., Case No. 1:12-cv-3005-WSD (Sept. 19, 2012) (Duffy, J.) (emphasis added). A true and correct copy is attached hereto as Exhibit 10.

51. On September 17, 2013, LabMD filed an answer challenging the FTC's jurisdiction and violations of LabMD's federal constitutional due process rights, among other things.

52. In September 2013, HHS said that it decided against even investigating LabMD's alleged PHI data-security practices, noting that it had not received any complaints.

53. On October 24, 2013, Mr. Sheer of the FTC served a subpoena duces tecum on Mr. Daugherty, LabMD's CEO and President, requesting the following documents concerning Mr. Daugherty's book:

- "All drafts of . . . [Mr. Daugherty's book about the FTC] that were reviewed by any third party prior to the Manuscript's publication."
- "All comments received on drafts of" Mr. Daugherty's book about the FTC.
- "All documents related to the source material for drafts of" Mr. Daugherty's book about the FTC, "including documents referenced or quoted in the" book.
- "All promotional materials related to" Mr. Daugherty's book criticizing the FTC, "including, but not limited to, documents posted on social media, commercials featuring . . . [Mr. Daugherty], and presentations or interviews given by" Mr. Daugherty.

54. After over four years of investigation and litigation, LabMD still does not know when or what it did "wrong" and cannot even determine what the elements of a data-security "unfairness" offense are in this case.

55. For example, FTC enforcement staff have refused to substantively respond to LabMD's interrogatories regarding PHI data-security standards—including "data-security standards, regulations, and guidelines the FTC seeks to enforce against LabMD"—except to cross-reference their response to LabMD's request that they produce "[a]ll documents sufficient to show the standards or criteria the FTC used in the past and is currently using to determine whether an entity's data-security practices violate Section 5 of the Federal Trade Commission Act from 2005 to the present."

56. Indeed, Complaint Counsel even objected to LabMD's interrogatory inquiring what "data-security standards, regulations, and guidelines the FTC will use to determine whether LabMD's data-security practices were not reasonable and appropriate" on the ground that it seeks opinions by undisclosed nontestifying experts and "calls for expert opinions."

57. The thousands of pages of materials that FTC enforcement staff have produced to LabMD in response to the foregoing document request (most of which was produced on March 3, 2014, two days before the close of fact discovery) consist almost exclusively of: Power Point presentations; FTC staff reports; emails; FTC Consumer Alerts, OnGuard posts, Guides for Business, FTC Office of Public Affairs blog posts, and assorted other Internet postings; materials FTC staff employees apparently use to prepare for presentations, including handwritten notes; copies of

FTC administrative complaints, draft administrative complaints, consent orders, and related documents; letters the FTC has sent to various companies; documents related to various FTC workshops; speeches given by various FTC Commissioners; assorted congressional testimony; and other miscellaneous materials. Some of these materials are of very recent vintage and dated after the events described in the FTC's August 2013 administrative complaint allegedly occurred. Some of these materials are dated after August 28, 2013, when the FTC issued this complaint. The only regulations that FTC enforcement staff produced to LabMD do not apply to LabMD and implement statutes that also do not apply to LabMD.

58. On March 3, 2014, FTC enforcement staff refused to admit, among other things, that the FTC's administrative complaint does not specifically reference any industry standards for data-security practices, hardware or software necessary to avoid a violation of Section 5, instead claiming that LabMD was asking for "an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside of the scope of discovery" and, in the alternative, denying that they were required to allege this.

59. FTC enforcement staff have even argued that "STANDARDS USED TO ENFORCE SECTION 5 ARE OUTSIDE THE SCOPE OF DISCOVERY," saying that "[t]he orders and opinions of the Commission and of th[e ALJ] …

preclude such discovery." Complaint Counsel's Motion for Protective Order Regarding Rule 3.33 Notice of Deposition, *In the Matter of LabMD*, FTC Dkt. No. 9357, at 7 (Feb. 14, 2014).

60. More recently, on March 18, 2014, FTC enforcement staff produced an expert witness report that for the first time—after more than four years of investigation and litigation—gave LabMD some notice as to what a FTC expert thinks LabMD did wrong. But that report did not even purport to assess LabMD's PHI data-security practices against any objective, applicable medical-industry data-security statute, regulation, custom, or standard.

III. LabMD Challenges The FTC's Jurisdiction.

61. On November 12, 2013, LabMD filed a dispositive Motion to Dismiss raising pure issues of law and questions of statutory interpretation in the FTC's administrative case. A true and correct copy is attached hereto as Exhibit 11. LabMD requested oral argument. Under the FTC's Rules of Practice, Commissioners (and not the ALJ) rule on dispositive motions to dismiss complaints they recently voted to issue in the first instance.

62. On November 14, 2014, LabMD also filed a Verified Complaint in the U.S. District Court for the District of Columbia seeking solely injunctive and

declaratory relief. LabMD v. FTC et al., Case No. 1:13-cv-01787-CKK, Dkt. No. 1 (D.D.C. Nov. 14, 2013).

63. On November 18, 2013, LabMD filed a petition for review in the U.S. Court of Appeals for the Eleventh Circuit, LabMD, Inc. v. FTC, Case No. 13-14267-F (11th Cir. Nov. 18, 2013). Ex. 1.

64. On November 25, 2013, LabMD filed an administrative stay motion in the FTC enforcement action.

65. On December 2, 2013, LabMD filed a reply in support of its administrative motion to dismiss. A true and correct copy is attached hereto as Exhibit 12.

66. On December 13, 2013, the FTC issued an order denying LabMD's stay motion ("December 13 Order"). A true and correct copy is attached hereto as Exhibit 13. The December 13 Order states that no Article III court has jurisdiction over LabMD's claims until the FTC gives its permission.

67. On December 16, 2013, the Eleventh Circuit issued two jurisdictional questions to the parties. Jurisdictional Questions, LabMD v. FTC, Case No. 13-15267-F (Dec. 16, 2013).

68. On December 23, 2013, LabMD filed a stay motion in in the Eleventh Circuit. Petitioner's Motion for Stay Pending Review, LabMD v. FTC, Case No. 13-15267-F (Dec. 23, 2013).

69. On January 16, 2014, the FTC denied LabMD's administrative Motion to Dismiss, rejecting LabMD's jurisdictional and fair-notice due process challenges without oral argument, thereby denying LabMD an opportunity to create a record (the "January 16 Order"). Ex. 2.

70. On January 17, 2014, the FTC submitted the January 16 Order to the Eleventh Circuit, via what it called a "notice of supplemental authority."

71. FTC did the exact same thing on the exact same day in FTC v. Wyndham Worldwide Corp. et al., Case No. 2:13-cv-01887-ES-SCM, Dkt. No. 151 (D. N.J. Jan. 17, 2014). The FTC claimed its order had the force of law and should be given deference under "Chevron." Ex. 3 at 6.

72. The FTC admits that it cannot and does not enforce HIPAA or HITECH. Ex. 2 at 12 & n.19.

73. The FTC admits that its case against LabMD solely alleges statutory Section 5 statutory "unfairness" violations, not "violations of the FTC's Health Breach Notification Rule." Id. at 20 n.20.

74. The FTC admits that it has failed to establish any data-security standards with the force of law that give notice as to what PHI data-security practices the Commission and its enforcement staff believes Section 5 forbids or requires. Ex. 2 at 15.

75. The FTC admits that it did not claim data-security regulatory authority until years after 1994, when Section 5 was last amended to add subsection (n). 15 U.S.C. § 45(n). Ex. 2 at 4, 8-9. Subsection (n) does not mention "data security," let alone explain what data-security practices the FTC believes Section 5 to forbid or require.

76. Yet the FTC claims subsection (n) gives fair notice: "Here, the three-part statutory standard governing whether an act or practice is 'unfair,' set forth in Section 5(n) [15 U.S.C. § 45], should dispel LabMD's concern about whether the statutory prohibition of 'unfair . . . acts or practices' is sufficient to give fair notice of what conduct is prohibited." Ex. 2 at 16.

77. The FTC's January 16 Order essentially asserts that constitutional fair-notice due process requirements are somehow inapplicable here because, according to the Defendant, the FTC is not pursuing "criminal punishment or civil penalties for past conduct." Ex. 2 at 16.

78. The FTC also claims it is not obligated to provide any fair notice at all of the PHI data-security practices it believes Section 5 to forbid or require because agencies have broad "discretion" to "address an issue by rulemaking or adjudication." Ex. 2 at 15.

79. For that matter, the FTC effectively claims that the standard for Section 5 "unfairness" PHI data-security liability is whether a company's practices are "unreasonable" according to it, while acknowledging that this is a case of first impression as to what is "unreasonable."

80. Elsewhere, the FTC admitted that there is no process through which businesses could have obtained guidance or an advisory opinion from the Commission regarding data-security practices. See Hearing Trans., FTC v. Wyndham et al., Case No. 2:13-cv-01887-ES-SCM, 52:10-11 (Nov. 7, 2012). A true and correct copy of an excerpt of the foregoing transcript is attached hereto as Exhibit 14 and is incorporated herein by reference.

81. On February 18, 2014, the Eleventh Circuit dismissed LabMD's Petition for Review and denied all pending motions as moot because there was no cease and desist order reviewable under 15 U.S.C. § 45(c). Instead, it ruled this Court has original jurisdiction over LabMD's ultra vires, statutory, and constitutional claims to

the extent that such claims could be asserted before a cease and desist order is entered. Ex. 1.

82. Therefore, on February 19, 2014, LabMD filed a Notice of Voluntary Dismissal Without Prejudice of LabMD v. FTC et al., Case No. 1:13-cv-01787-CKK, Dkt. No. 20 (D.D.C.), because under D.C. Circuit law, which is different from the law of this Circuit, only the U.S. Court of Appeals for the D.C. Circuit has jurisdiction over those claims, yet the D.C. Circuit will never have jurisdiction under 15 U.S.C. § 45(c) because LabMD has not done business there.

83. The FTC has issued a final agency decision regarding jurisdiction, and LabMD has exhausted all administrative remedies with respect to its jurisdictional and constitutional fair-notice due process arguments.

IV. The FTC Denies LabMD Procedural Due Process.

84. To begin with, the FTC has never specified the PHI data-security standards LabMD failed to meet, thereby denying LabMD an opportunity to effectively defend itself and granting the Commission, Mr. Sheer, and other federal bureaucrats unlimited discretion to decide what is "unreasonable" after the fact and to regulate the entire health care industry based on their idiosyncratic whim, caprice, and fancy.

85. In 2009, the FTC modified its Rules of Practice to deny respondents a fair defense and to render motion practice futile. 74 Fed. Reg. 20,205 (May 1, 2009).

86. At the initial pretrial conference, the ALJ told LabMD's counsel:

> [L]et me talk about dispositive motions . . . . There is a rule that covers that, if you intend to file a summary judgment, and if you don't know, I'll tell you. Summary judgments will be ruled on by the Commission, the same body that voted to issue the complaint in this case. With respect to motion to dismiss or other substantive motion, the rules provide that if they are filed before the start of the evidentiary hearing, they will be ruled on by that same Commission . . . .

Ex. 9 at 18:11-15. The ALJ lacks power to even grant a continuance of the evidentiary hearing or stay the proceedings pending adjudication of dispositive motions before the Commission. See 16 C.F.R. §§ 3.22(b), 3.41(b).

87. The FTC was extensively warned about the constitutional implications of its power-grab during the comment period.

88. The American Bar Association (ABA) Section of Antitrust Law ("Antitrust Section") said the revisions forced respondents to address prehearing issues to the FTC without the benefit of a prior opinion authored by a party who was not involved in crafting and approving a complaint. Comments of the ABA Section of Antitrust Law in Response to the Federal Trade Commission's Request for Public Comment Regarding Parts 3 and 4 Rules of Practice Rulemaking—P072194, at 4 (Nov. 6, 2008).

89. The Antitrust Section explained that its "primary concern is that by 'codifying' the Commission's right to interject itself into prehearing case management, it may undermine the integrity of the process, compromise the ALJ, and create an appearance of unfairness." Id. at 12. The Antitrust Section also said the FTC's amendments "could reduce the quality of decision making, and may color the perception of the fairness and impartiality of Commission proceedings—a particularly important issue considering that when hearing an appeal, federal courts will give deference to a final FTC decision." Id. at 11.

90. The U.S. Chamber of Commerce added that "it appears that the proposed changes are being rushed into place and for the purpose of giving the FTC material, tactical, and procedural advantage . . . ." U.S. Chamber of Commerce, Comment, Re: Parts 3 and 4 Rules of Practice Rulemaking—P072104, at 1 (Nov. 6, 2008). In fact:

> The FTC's proposed regulations work to effectively eliminate the role of the independent Administrative Law Judge (ALJ) to manage and prepare an initial decision for a case. This results in the elimination of a vital check on potential unfairness inherent in the FTC's administrative procedure. Under the FTC's process, the Commissioners act as both prosecutor and judge in administrative trials. Thus, the same individuals who decide to issue the complaint also decide the final appeal of the administrative trial. With such a clear potential for unfairness or conflict of interest at the forefront of FTC administrative adjudication, it is necessary to preserve some sort of fairness check.

Id. at 2.

91. Under current Commission Rule 3.22(a), "[m]otions to dismiss filed before the evidentiary hearing, motions to strike, and motions for summary decision shall be directly referred to the Commission and shall be ruled on by the Commission unless the Commission in its discretion refers the motion to the Administrative Law Judge."

92. In excess of their authority and in violation of the Constitution's guarantee of due process, the FTC has assumed for itself the power to legislate, to prosecute, and to judge LabMD without even specifying in advance the elements of the data-security offense LabMD has allegedly committed.

93. The empirical evidence demonstrates that the FTC's administrative process is a rigged exercise in futility for LabMD and others similarly situated.

94. According to Commissioner Wright:

> The FTC has voted out a number of complaints in administrative adjudication that have been tried by administrative law judges ("ALJs") in the past nearly twenty years. In each of those cases, after the administrative decision was appealed to the Commission, the Commission ruled in favor of FTC staff. In other words, in 100 percent of cases where the ALJ ruled in favor of the FTC, the Commission affirmed; and in 100 percent of the cases in which the ALJ ruled against the FTC, the Commission reversed.

Joshua D. Wright, Comm'r, Fed. Trade Comm., Recalibrating Section 5: A Response to the CPI Symposium, CPI Antitrust Symposium, at 4 (November 2013), available at

http://www.ftc.gov/sites/default/files/documents/public_statements/recalibrating-section-5-response-cpi-symposium/1311section5.pdf (last visited Mar. 18, 2014).

95. Further administrative proceedings are exhausted and futile.

V. The Irreparable Harm Done By The FTC To LabMD.

96. FTC's power-grab has destroyed LabMD's customer relationships and, in large measure, driven LabMD to cease accepting new specimen samples. But for all of the time, attention, and money LabMD has been forced to devote to addressing the FTC's actions, the company would almost certainly be accepting new specimen samples and providing cancer-diagnostic services to doctors to this day.

97. LabMD, and its doctors, have been denied insurance coverage as a direct result of the FTC's ongoing persecution of the company. For example, One Beacon (a medical malpractice insurance company) recently denied LabMD, and its doctors, coverage, saying: "[W]e are unable to offer ERP terms for the entity [LabMD], and as a result, the individual physicians so I will be closing the file. The potential volatility due to the FTC investigation is something we want to stay away from particularly because it pertains to medical records."

98. LabMD's general liability insurance carrier is planning to non-renew its insurance policy effective May 6, 2014.

99. The FTC's personnel have intentionally interfered with LabMD's customer relationships and effectively engaged in a campaign of commercial disparagement.

100. The FTC's actions have caused, and continue to cause, irreparable injury to LabMD's business reputation and good will in the marketplace.

101. The FTC, Mr. Sheer, and other FTC employees have intentionally set out to destroy LabMD's commercial brand, reputation, and good will.

102. The FTC, Mr. Sheer, and others have caused and continue to cause LabMD irreparable harm far beyond mere litigation expenses and threaten the viability of LabMD's business operations. Much of this harm cannot be quantified in monetary terms, and cannot be remedied by monetary damages. For example, on January 6, 2014, LabMD notified its customers that it would no longer be accepting new specimen samples for testing for the foreseeable future, effective January 11, 2014.

CLAIMS FOR RELIEF

First Claim for Relief
(For Violation of the APA)

103. LabMD repeats paragraphs 4-5, 8-10, 16-19, 21-22, 27-32, 41-50, 54-61, 64-66, 69-81, 84, and 93-95.

104. The FTC's action against LabMD is arbitrary, capricious, an abuse of discretion and power, in excess of statutory authority and short of statutory right, and contrary to law and constitutional right, in violation of 5 U.S.C. § 706.

105. The FTC does not have jurisdiction to regulate LabMD's patient-information data-security and thus its actions are ultra vires.

106. The Commission's orders denying the jurisdictional, ultra vires, and due process claims raised in LabMD's motion to dismiss and LabMD's motion for a stay are both "final agency actions" within the meaning of 5 U.S.C. § 704 and thus LabMD's APA claims are ripe and reviewable now. TVA v. Whitman, 336 F.3d 1236, 1248 (11th Cir. 2004); see, e.g., CSI Aviation Servs. v. DOT, 637 F.3d 408, 411-14 (D.C. Cir. 2011); see Sackett, 132 S. Ct. at 1371-72; see also Athlone Indus., Inc. v. CPSC, 707 F.2d 1485, 1487-88 (D.C. Cir. 1983).

107. LabMD has exhausted all administrative remedies with respect to its jurisdictional and constitutional due-process arguments, which the Commission formally rejected on January 16, 2014.

108. In addition, only administrative remedies providing a genuine opportunity for adequate relief need be exhausted, and here exhaustion is also independently not required because the administrative process is futile and inadequate and LabMD will continue to suffer irreparable harm unless its claims are reviewed by

an Article III Court now. See N.B. by D.G. v. Alachua Cnty. Sch. Bd., 84 F.3d 1376, 1379 (11th Cir. 1996); Porter v. Schweiker, 692 F.2d 740, 742-43 (11th Cir. 1982); Randolph-Sheppard Vendors of Am. v. Weinberger, 795 F.2d 90, 107-08 (D.C. Cir. 1986) (irreparable harm excuses exhaustion).

109. Therefore, the FTC's enforcement action against LabMD should be enjoined and a declaration issued that it lacks authority to regulate patient information data-security.

Second Claim for Relief
(For Ultra Vires Agency Action)

110. LabMD repeats paragraphs 4-5, 8-10, 16-19, 21-22, 27-32, 41-50, 61, 70-81, and 93-96.

111. Regardless of the presence vel non of "final agency action" under 5 U.S.C. § 704, this Court has jurisdiction to adjudicate LabMD's nonstatutory ultra vires and constitutional claims, for the presence or absence of "final agency action" has no jurisdictional effect. See, e.g., Trudeau v. FTC, 456 F.3d 178 (D.C. Cir. 2006); Muniz-Muniz v. U.S. Border Patrol, No. 12-4419, 2013 U.S. App. LEXIS 25400, at *11 (6th Cir. Dec. 20, 2013) (noting that "all of our sister circuits" have concluded 5 U.S.C. § 704 has no effect on a federal-question jurisdiction to adjudicate non-APA claims); see also Arbaugh v. Y & H Corp., 546 U.S. 500, 511, 516-17 (2006).

112. Thus, the FTC's ultra vires actions are ripe for judicial review now regardless of the reviewability of LabMD's APA claims.

113. Exhaustion is not required for these claims under any circumstances. See XYZ Law Firm v. FTC, 525 F. Supp. 1235, 1237 (N.D. Ga. 1981).

114. The FTC's actions against LabMD exceed the power given to it in Section 5 and are thus ultra vires.

115. Judicial review of this claim is available because the Defendant's ultra vires actions exceed the authority conferred on it by Congress and the United States Constitution.

116. Moreover, inter alia, the FTC has effectively violated three specific and mandatory restraints on its Section 5 "unfairness" power.

117. First, the FTC's abuse exceeds its delegated powers and is contrary to specific the FTC Act's prohibitions on the use of consent orders and speeches to create a binding "common law" of data security. 15 U.S.C. § 45(m)(1)(B).

118. Second, in addition to the fact that Congress has not given the FTC Section 5 "unfairness" authority to regulate data security, let alone authority to over-file HHS and regulate PHI data security, the FTC has also independently violated 15 U.S.C. § 45(n)'s specific limits on its Section 5 "unfairness" authority. 15 U.S.C. § 45(n) explicitly states that the Defendant "shall have no authority under this section

or section 18 [15 U.S.C. § 57a] to declare unlawful an act or practice on the grounds that such act or practice is unfair" under the circumstances of this case. 15 U.S.C. § 45(n) further explicitly bars the FTC from using its public policy views as a primary basis for exercising its unfairness authority.

119. Third, the FTC's sworn responses to LabMD's discovery requests demonstrate it is seeking to enforce against LabMD random Internet postings, e-mail alerts, Commission staff reports, and congressional testimony they say establish data-security standards LabMD should have followed, even those these documents do not have the force of law and were not even published in the Federal Register, and they do not allege that LabMD had actual knowledge of any of these Internet postings and other materials. 5 U.S.C. § 552(a)(1).

120. FTC's unauthorized actions are the direct and proximate cause of LabMD's injuries, as described above. Therefore, LabMD is entitled to the declaratory and injunctive relief requested herein.

Third Claim for Relief
(For Fair-Notice Due Process Violations)

121. LabMD repeats paragraphs 4-5, 7-10, 46-49, 74-80, 84-85, and 118-119.

122. This Court has jurisdiction over LabMD's fair-notice due process claim now. Exhaustion is not required for these claims under any circumstances.

123. The Fifth Amendment to the United States Constitution states that "[n]o person shall be . . . deprived of life, liberty, or property, without due process of law." U.S. Const. amend. V.

124. The draft notice order ("Commission Notice Order") if made effective, will be in place for twenty (20) years and, inter alia, require LabMD to (1) "establish and implement, and thereafter maintain, a . . . security program"; (2) "obtain initial and biennial assessment and reports" from third parties for a period of twenty (20) years; (3) provide Commission-approved notice to the individuals listed in the accounts-receivable file and their health insurance companies of Tiversa's actions via first-class mail; (4) deliver copies of the Commission Notice Order to "current and future principals, officers, directors, and mangers," as well as deliver copies to many current and future employees, agents, representatives, and business entities; (5) notify the FTC in writing at least thirty (30) days before making numerous changes, such as change in corporate name or address; and (6) prepare and file detailed reports with the FTC.

125. Additionally, the FTC has reserved the right to order such other relief as it finds necessary and appropriate if it decides that the Commission Notice Order is insufficient, including seeking "restitution" and other types of relief authorized by Section 19 of the Federal Trade Commission Act, 15 U.S.C. § 57b (civil actions for

violations of rules and cease and desist orders respecting unfair or deceptive acts or practices), including but not limited to rescission or reformation of contracts and payment of monetary damages.

126. Under 15 U.S.C. § 45(l), each violation of the FTC cease and desist orders carries up to a $10,000 civil penalty.

127. FTC's actions, January 16 Order, December 13 Order, and the Commission Complaint and Notice Order, thus implicate LabMD's property rights, which are protected by the Due Process Clause of the Fifth Amendment.

128. FTC's refusal to promulgate any regulations or to issue any other guidelines clarifying and providing any notice, let alone constitutionally adequate notice, of what data-security practices they believe Section 5 forbids or requires, or to otherwise establish any meaningful standards, violates LabMD's due process rights.

129. Due process requires that laws that 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); Connally v. Gen. Constr. Co., 269 U.S. 385, 391-95 (1926).

130. This constitutional fair-notice requirement has been thoroughly incorporated into administrative law to limit agencies' ability to regulate past conduct through after-the-fact enforcement actions. Georgia Pac. Corp. v. OSHRC, 25 F.3d 999, 1005 (11th Cir. 1994). Fair-notice due process requirements thus apply to the

FTC administrative enforcement actions seeking to impose cease and desist orders for alleged violations of Section 5.

131. The FTC has failed to meet its burden of establishing reasonably ascertainable standards for what data-security practices it believes Section 5 to either forbid or to require. See Georgia Pac. Corp., 25 F.3d at 1005; Trinity Broad. of Fla., Inc. v. FCC, 211 F.3d 618, 628-32 (D.C. Cir. 2000).

132. Basic principles of due process limit the FTC's "discretion" to enforce Section 5 through administrative adjudications; specifically, the FTC can proceed by adjudication only if it has already provided the baseline level of fair notice that the Constitution requires. The FTC has failed to provide LabMD the baseline level of fair notice of the data-security practices it believes to be required or forbidden by Section 5's "unfairness" language.

133. Because the FTC's Section 5 PHI data-security regulatory scheme forbids or requires the doing of an act in terms so vague that men and women of common intelligence must necessarily guess at its meaning and differ as to its application, it violates due process.

134. In addition, even if the FTC's "reasonableness" standard for PHI data security otherwise passed constitutional muster, the FTC's failure to link its data-security standards to medical-industry standards independently violates due process.

135. FTC's pattern and practice of fair-notice due process violations, as applied to LabMD and all similarly situated, including the defendants in FTC v. Wyndham, violates due process.

Fourth Claim for Relief
(For Facial, Structural Due Process Violations)

136. LabMD repeats paragraphs 4-5, 7-10, 17-19, 23-34, and 84-96.

137. Exhaustion of administrative remedies is not required for facial and structural due process challenges. See, e.g., Matthews v. Eldridge, 424 U.S. 319, 329-32 (1976); Amos Treat & Co. v. SEC, 306 F.2d 260, 267 (D.C. Cir. 1963).

138. The substantial private interests affected by the FTC's actions, the high risk of erroneous deprivation of LabMD's property interests, and the high value of additional procedural safeguards outweigh the FTC's de minimis interest in the existing procedures. Therefore, LabMD has not been provided the procedural safeguards that it is constitutionally entitled to have.

139. Due process minimally requires a fair trial in a fair tribunal and "this applies to administrative agencies which adjudicate as well as to courts." Withrow v. Larkin, 421 U.S. 35, 46-47 (1975).

140. FTC's modifications to its Rules of Practices transgress constitutional limits on blending of prosecutorial, legislative, and adjudicative functions and deprive

all respondents of a fair administrative hearing. Therefore, the Commission's Rules facially and structurally violate due process.

141. Furthermore, the FTC's ex post facto enforcement action against LabMD for alleged violations of unspecified data-security standards in a proceeding in which the FTC acts in a legislative, prosecutorial, and adjudicative capacity further violates due process.

142. Finally, the FTC has predetermined this matter, denying LabMD its right to a fair and level review, including a fair hearing on its Motion to Dismiss before an impartial ALJ.

143. FTC's intentional violations of LabMD's due process rights has caused LabMD hundreds of thousands of dollars in actual damages, harmed its business reputation, caused it to lose good will and business opportunities, and brought the company to the brink of ruin.

Fifth Claim for Relief

(For Retaliation Against LabMD for Protected First Amendment Speech)

144. LabMD repeats paragraphs 4-5, 7-11, 23-49, and 53.

145. The First Amendment to the United States Constitution guarantees LabMD freedom of speech.

146. Mr. Daugherty's book, his webpage about the book, and his speeches and statements about the FTC's actions are political speech and speech about matters of public concern and thus protected by the First Amendment.

147. On information and belief, the FTC's actions against LabMD were retaliation for protected speech by Mr. Daugherty.

148. The FTC's actions against LabMD, as set forth herein, will likely chill a person of ordinary firmness from engaging in the protected First Amendment activity.

149. On information and belief, the FTC's conduct herein was precisely intended and designed, at least in part, to punish LabMD and chill government criticism by LabMD and others targeted by the government.

150. Even if the FTC, Complaint Counsel, and other FTC employees disagree with and find Mr. Daugherty's statements about their actions to be patently offensive, they are not allowed retaliate by bringing an enforcement action against LabMD.

RELIEF REQUESTED

WHEREFORE LabMD requests the following relief:

A. That the Court enter a declaratory judgment that (1) the FTC lacks statutory authority to regulate patient-information data-security practices under Section 5; (2) the FTC's efforts to regulate patient information are ultra vires; (3) the FTC violated LabMD's due process rights by failing to provide constitutionally

adequate notice of what data-security practices the Commission believed Section 5 to forbid or require before the Complaint was filed; (4) the FTC violated LabMD's due process rights by unconstitutionally combining legislative, prosecutorial, investigative, and adjudicatory functions by, among other things, allowing FTC Commissioners to rule on dispositive motions concerning complaints they recently voted to issue; and (5) the FTC unconstitutionally retaliated against LabMD for engaging in constitutionally protected speech.

B. That the Court enter preliminary and permanent injunctive relief providing that the FTC, its agents, servants, employees, and attorneys, and anyone who is in active concert or participation with any of them, shall take no further actions in connection with administrative proceedings known as In the Matter of LabMD, FTC Dkt. No. 9357, including but not limited to issuing orders, holding hearings, taking discovery, and filing motions.

C. That the Court enter preliminary and permanent injunctive relief providing that the FTC, its agents, servants, employees, and attorneys, and anyone who is in active concert or participation with any of them, shall not (1) initiate any civil or administrative enforcement action against LabMD or any other person on the ground that their patient information data-security practices are "unfair" in violation of Section 5; (2) investigate whether LabMD's or any other person's patient

information data-security practices violate Section 5 for "unfairness"; (3) attempt to establish substantive data-security standards under Section 5 and/or enforce Section 5 in civil or administrative proceedings; or (4) undertake or pursue any administrative enforcement proceedings until the Commission amends its Rules of Practice to provide constitutionally adequate due process.

D. That the Court award LabMD its attorneys' fees and litigation costs under the Equal Access to Justice Act and/or such other applicable law.

E. Such other and further relief as this Court deems just and proper.

Respectfully submitted, this 20th day of March, 2014.

/s/ Ronald L. Raider

KILPATRICK TOWNSEND
& STOCKTON LLP
1100 Peachtree Street, NE
Suite 2800
Atlanta, Georgia 30309
Telephone (404) 815-6500
Facsimile (404) 815-6555
rraider@kilpatricktownsend.com
bsingleton@kilpatricktownsend.com
bmeyer@kilpatricktownsend.com

Ronald L. Raider
Georgia Bar No. 592192
Burleigh L. Singleton
Georgia Bar No. 649084
William D. Meyer
Georgia Bar No. 950008

Counsel for Plaintiff

OF COUNSEL:

Reed D. Rubinstein
(applying for admission pro hac vice)
D.C. Bar No. 440153
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9120
Fax: 202.372.9141
reed.rubinstein@dinsmore.com

Senior Vice President for Litigation and Counsel to Cause of Action

Michael D. Pepson
(applying for admission pro hac vice)
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and administrative proceedings before federal agencies.

Dated: March 20, 2014

Verification

I am Michael Daugherty, owner and CEO of LabMD, Inc., which is the plaintiff in this action.

I have read the foregoing Complaint and verify and declare on behalf of LabMD, Inc., under penalty of perjury, that its factual allegations are true, except to those matters stated on information and belief, and as to those matters I believe them to be true to the best of my knowledge.

LabMD, Inc.

By: _____ Date: 3/19/14
Michael Daugherty

LOCAL RULE 7.1 CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing pleading filed with the Clerk of Court has been prepared in 14 point Times New Roman font in accordance with Local Rule 5.1(C).

Dated: March 20, 2014.

/s/ Ronald L. Raider
Ronald L. Raider

EXHIBIT 1

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT

No. 13-15267-F

LABMD, INC.,

Petitioner,

versus

FEDERAL TRADE COMMISSION,

Respondent.

Petitions for Review of a Decision of the
Federal Trade Commission

Before: HULL, MARCUS, and WILSON, Circuit Judges.

BY THE PANEL:

This petition for review is DISMISSED, *sua sponte*, for lack of jurisdiction. All pending motions are DENIED as moot. Petitioner LabMD, Inc. claims that we can hear its petition either under 15 U.S.C. § 45(c), or as an independent Administrative Procedure Act ("APA"), *ultra vires*, or constitutional claim. 15 U.S.C. § 45(c) only gives courts of appeals authority to review "an order of the [Federal Trade] Commission to cease and desist from using any method of competition or act or practice." There is no such order here, and no authority suggests that our granted authority extends beyond review of such cease and desist orders. Because federal courts are courts of limited jurisdiction and possess only that power authorized by Constitution and statute, we lack jurisdiction to hear the petition for review under that section. *See Kokkonen v.*

Guardian Life Ins. Co. of Am., 511 U.S. 375, 377, 114 S. Ct. 1673, 1675, 128 L. Ed. 2d 391 (1994).

With respect to any APA, *ultra vires*, or constitutional claims that may be lurking in this petition for review, we do not have original jurisdiction to hear these claims, regardless of whether, as petitioner asserts, the actions the Federal Trade Commission has taken amount to reviewable agency action even if not reviewable under § 45(c). The APA itself does not confer subject matter jurisdiction upon any court. *See Califano v. Sanders*, 430 U.S. 99, 107, 97 S.Ct. 980, 985, 51 L.Ed.2d 192 (1977). Rather, jurisdiction to hear suits under the APA is conferred by 28 U.S.C. § 1331, which provides district courts original jurisdiction of all civil actions arising under the laws of the United States. *See id.* at 105, 97 S.Ct. at 984; *see also Sierra Club v. Martin*, 110 F.3d 1551, 1554 n.11 (11th Cir. 1997). Any APA, *ultra vires*, and constitutional claims, to the extent they can be asserted at this stage, first must be asserted and considered in a district court. We do not express or imply any opinion about whether a district court has jurisdiction to hear such claims or about the merits of those claims.

No motion for reconsideration may be filed unless it complies with the timing and other requirements of 11th Cir. R. 27-2 and all other applicable rules.

EXHIBIT 2

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**

ORDER DENYING RESPONDENT LABMD'S MOTION TO DISMISS

By Commissioner Joshua D. Wright, for a unanimous Commission:[1]

This case presents fundamental questions about the authority of the Federal Trade Commission ("FTC" or "the Commission") to protect consumers from harmful business practices in the increasingly important field of data security. In our interconnected and data-driven economy, businesses are collecting more personal information about their customers and other individuals than ever before. Companies store this information in digital form on their computer systems and networks, and often transact business by transmitting and receiving such data over the Internet and other public networks. This creates a fertile environment for hackers and others to exploit computer system vulnerabilities, covertly obtain access to consumers' financial, medical, and other sensitive information, and potentially misuse it in ways that can inflict serious harms on consumers. Businesses that store, transmit, and use consumer information can, however, implement safeguards to reduce the likelihood of data breaches and help prevent sensitive consumer data from falling into the wrong hands.

Respondent LabMD, Inc. ("LabMD") has moved to dismiss the Complaint in this adjudicatory proceeding, arguing that the Commission has no authority to address private companies' data security practices as "unfair . . . acts or practices" under Section 5(a)(1) of the Federal Trade Commission Act ("FTC Act" or "the Act"), 15 U.S.C. § 45(a)(1). This view, if accepted, would greatly restrict the Commission's ability to protect consumers from unwanted privacy intrusions, fraudulent misuse of their personal information, or even identity theft that may result from businesses' failure to establish and maintain reasonable and appropriate data security measures. The Commission would be unable to hold a business accountable for its conduct, even if its data security program is so inadequate that it "causes or is likely to cause

[1] Commissioner Brill did not take part in the consideration or decision herein.

substantial injury to consumers [that] is not reasonably avoidable by consumers themselves and [such injury is] not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n).

LabMD's Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings ("Motion to Dismiss" or "Motion"), filed November 12, 2013, calls on the Commission to decide whether the FTC Act's prohibition of "unfair . . . acts or practices" applies to a company's failure to implement reasonable and appropriate data security measures. We conclude that it does. We also reject LabMD's contention that, by enacting the Health Insurance Portability and Accountability Act ("HIPAA") and other statutes touching on data security, Congress has implicitly stripped the Commission of authority to enforce Section 5 of the FTC Act in the field of data security, despite the absence of any express statutory language to that effect. Nor can we accept the premise underlying LabMD's "due process" arguments – that, in effect, companies are free to violate the FTC Act's prohibition of "unfair . . . acts or practices" without fear of enforcement actions by the Commission, unless the Commission has first adopted regulations. Accordingly, we deny LabMD's Motion to Dismiss.

PROCEDURAL BACKGROUND

On August 28, 2013, the Commission issued an administrative complaint ("Complaint") against LabMD, a Georgia-based company in the business of conducting clinical laboratory tests on specimen samples from consumers and reporting test results to consumers' health care providers. The Complaint alleges that LabMD engaged in "practices that, taken together, failed to provide reasonable and appropriate security for personal information on its computer networks," *see* Complaint, ¶ 10; that these practices caused harm to consumers, including exposure to identity theft and disclosure of sensitive, private medical information, *id.*, ¶¶ 12, 17-21; and, consequently, that LabMD engaged in "unfair . . . acts or practices" in violation of the FTC Act. *Id.*, ¶¶ 22-23. LabMD submitted its Answer and Affirmative Defenses to the Administrative Complaint ("Answer") on September 17, 2013.

LabMD filed its Motion to Dismiss on November 12, 2013.[2] On November 22, 2013, Complaint Counsel filed its Response in Opposition to Respondent's Motion to Dismiss Complaint with Prejudice ("CC Opp."). LabMD filed its Reply to Complaint Counsel's Response in Opposition to Respondent's Motion to Dismiss ("Reply") on December 2, 2013. Factual discovery is now underway and is scheduled to close on March 5, 2014. The evidentiary hearing before the Administrative Law Judge is scheduled to begin on May 20, 2014.

[2] The Commission issued an Order on December 13, 2013, denying both LabMD's request for a stay of the administrative proceedings pending resolution of its Motion to Dismiss (*see* Motion at 29-30) and a separate Motion for Stay Pending Judicial Review that LabMD filed on November 26, 2013.

STANDARD OF REVIEW

We review LabMD's Motion to Dismiss using the standards a reviewing court would apply in assessing a motion to dismiss for failure to state a claim.[3] *See* Fed. R. Civ. P. 12(b)(6); *see also* Motion at 8; CC Opp. at 3; *S.C. State Bd. of Dentistry*, 138 F.T.C. 230, 232-33 (2004); *Union Oil Co.*, 138 F.T.C. 1, 16 (2004). Under this framework, "[o]ur task is to determine whether the [Complaint] contains sufficient factual matter . . . to state a claim to relief that is plausible on its face." *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. 2010) (citation omitted). For purposes of this analysis, we "accept[] the allegations in the complaint as true and construe[] them in the light most favorable to [Complaint Counsel]." *Am. Dental Ass'n v. Cigna Corp.*, 605 F.3d 1283, 1288 (11th Cir. 2010).

ANALYSIS

I. THE COMMISSION HAS AUTHORITY TO ENFORCE THE FTC ACT BY ADJUDICATING WHETHER THE DATA SECURITY PRACTICES ALLEGED IN THE COMPLAINT ARE "UNFAIR."

LabMD contends that the Commission lacks statutory authority to regulate or bring enforcement action with respect to the data security practices alleged. Motion at 9-21. We disagree. As discussed below, the Commission's authority to protect consumers from unfair practices relating to deficient data security measures is well-supported by the FTC Act, is fully consistent with other statutes, and is confirmed by extensive case law.[4]

A. Congress Intended to Delegate Broad Authority to the Commission to Proscribe Activities that Qualify as "Unfair Acts or Practices."

LabMD's broadest argument is that Section 5 does not authorize the FTC to address *any* data security practices. *See, e.g.*, Motion at 10 ("even if Section 5 does authorize the FTC to

[3] The Commission's administrative adjudicatory proceedings are governed by the FTC Act and the Commission's Rules of Practice, rather than the rules and standards that govern federal courts. Nonetheless, "since many adjudicative rules are derived from the Federal Rules of Civil Procedure, the latter may be consulted for guidance and interpretation of Commission rules where no other authority exists." FTC Op. Manual § 10.7. Here, the most relevant provision in the Commission's Rules of Practice (16 C.F.R. § 3.11(b)(2)) is very similar to the analogous court rule (Fed. R. Civ. P. 8(a)(2)). Thus, in this instance, we exercise our discretion to apply the pleading standards summarized above.

[4] At some points in the Motion, LabMD frames its arguments as challenges to the scope of the Commission's "jurisdiction" (*e.g.*, at 1, 2, 8, 16, 18, 19), while elsewhere it acknowledges the Commission's "Section 5 'unfairness' authority" but asserts that we cannot apply such authority to LabMD's data security practices. *Id.* at 18. As the Supreme Court recently clarified, "there is *no difference*, insofar as the validity of agency action is concerned, between an agency's exceeding the scope of its authority (its 'jurisdiction') and its exceeding authorized application of authority that it unquestionably has." *City of Arlington v. FCC*, 133 S. Ct. 1863, 1870 (2013). This is because, "for agencies charged with administering congressional statutes[,] [b]oth their power to act and how they are to act is authoritatively prescribed by Congress." *Id.* at 1869; *see* Motion at 9.

regulate data-security, which it does not"); *id.* at 17 (asserting "the Commission's lack of power to regulate data security through its general Section 5 'unfairness' authority'"). Motion at 16. LabMD points out that "there is nothing in Section 5 explicitly authorizing the FTC to directly regulate . . . data-security practices." *Id.* at 20. Ignoring the facially broad reach of Section 5's prohibition of "unfair . . . acts or practices in or affecting commerce," LabMD urges the Commission to conclude from the absence of explicit "data security" authority in the FTC Act that the Commission has no such authority. *See, e.g.*, Motion at 14 ("When Congress has wanted the FTC to have data security authority, it has said so"); *id.* ("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."); *id.* at 16 ("Section 5 does not give the FTC the authority to regulate data-security practices as 'unfair' acts or practices"); *id.* at 21 ("Section 5 does not contain a clear and manifest statement from Congress to authorize the Commission's [authority over] data security"). The statutory text, legislative history, and nearly a century of case law refute LabMD's argument.

As the courts have long recognized, "[n]either the language nor the history of the [FTC] [A]ct suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories." *FTC v. R.F. Keppel & Bro., Inc.*, 291 U.S. 304, 310 (1934). Rather, the legislative history of the FTC Act confirms that Congress decided to delegate broad authority "to the [C]ommission to determine what practices were unfair," rather than "enumerating the particular practices to which [the term 'unfair'] was intended to apply. . . . There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 240 (1972) (quoting S. Rep. No. 597, 63d Cong., 2d Sess., 13 (1914), and H.R. Conf. Rep. No.1142, 63d Cong., 2d Sess., 19 (1914)). *See also Atl. Refining Co. v. FTC*, 381 U.S. 357, 367 (1965) (Congress "intentionally left development of the term 'unfair' to the Commission rather than attempting to define 'the many and variable unfair practices which prevail in commerce.'") (quoting S. Rep. No. 592, 63d Cong., 2d Sess., 13 (1914)).

This legislative history pertains to Congress' enactment of the prohibition of "unfair methods of competition" in 1914. Similar considerations motivated Congress's reuse of the same broad term ("unfair") when it amended the statute in 1938 to proscribe "unfair and deceptive acts and practices" as well as "unfair methods of competition." The 1938 amendment perpetuated and expanded the broad congressional delegation of authority to the Commission by "overturn[ing] . . . attempts [in some court decisions] to narrowly circumscribe the FTC's authority." *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 966 (D.C. Cir. 1985). Congress thus clarified that "the Commission can prevent such acts or practices which injuriously affect the general public as well as those which are unfair to competitors." *Id.* (quoting H.R. Rep. No. 1613, 75th Cong., 1st Sess. 3 (1937)).

As LabMD points out (*see* Motion at 18), Congress enacted legislation in 1994 that provided a sharper focus for the application of the Commission's "unfairness" authority, by amending the FTC Act to incorporate three specific criteria governing the application of "unfair . . . acts or practices" in adjudicatory and rulemaking proceedings. Specifically, the new Section 5(n) of the Act provides that, in enforcement actions or rulemaking proceedings, the Commission has authority to determine that an act or practice is "unfair" if that act or practice

"[1] causes or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. 45(n). These criteria, derived from the Commission's pre-existing *Policy Statement on Unfairness*, codified the analytical framework that the Commission already had been applying for the preceding decade in its efforts to combat "unfair . . . acts or practices." *See* Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980) ("*Policy Statement on Unfairness*"), *reprinted in Int'l Harvester Co.*, 104 F.T.C. 949, 1070, 1073 (1984). Section 5(n)'s specific criteria provide greater certainty for businesses by setting forth the factors to be used to evaluate whether their acts or practices are "unfair." That fact alone refutes LabMD's contention that the "general statutory terms" in Section 5 are too "vague" to be applied to the conduct alleged in the Complaint. *See* Motion at 19.

At the same time, Congress, in enacting Section 5(n), confirmed its intent to allow the Commission to continue to ascertain, on a case-by-case basis, which specific practices should be condemned as "unfair." Thus, to this day, "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*, 767 F.2d at 966.

The Commission and the federal courts have been applying these three "unfairness" factors for decades and, on that basis, have found a wide range of acts or practices that satisfy the applicable criteria to be "unfair," even though – like the data security practices alleged in this case – "there is nothing in Section 5 explicitly authorizing the FTC to directly regulate" such practices (*see* Motion at 20). *See, e.g., FTC v. Neovi, Inc.*, 604 F.3d 1150, 1155 (9th Cir. 2010) (creating and delivering unverified checks that enabled fraudsters to take unauthorized withdrawals from consumers' bank accounts); *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1193 (10th Cir. 2009) (covert retrieval and sale of consumers' telephone billing information); *Orkin Exterminating Co. v. FTC*, 849 F.2d 1354, 1364 (11th Cir.1988) (unilateral breach of standardized service contracts); *Am. Fin. Servs. Ass'n*, 767 F.2d at 971 (oppressive litigation conduct to repossess household goods sold on credit).

LabMD cites *American Bar Association v. FTC*, 430 F.3d 457 (D.C. Cir. 2005), for the proposition that the Commission is overstepping the bounds of its authority to interpret the FTC Act. *See* Motion at 20. But that case is inapposite. *ABA* concerned the agency's determination, in construing the Gramm-Leach-Bliley Act ("GLB Act"), that attorneys fell within that statute's definition of "financial institutions" – a defined term that, in turn, incorporated by reference a set of lengthy and detailed definitions imported from other statutes and other agencies' regulations. The court found it "difficult to believe" that, in enacting a statutory "scheme of the length, detail, and intricacy of the one" under review, Congress could have left sufficient remaining ambiguity, "hidden beneath an incredibly deep mound of specificity," to support imposing GLB Act requirements upon "a profession never before regulated by federal [financial service] regulators, and never mentioned in the statute." 430 F.3d at 469. By contrast, the statutory text at issue in this case – "unfair . . . acts or practices" – conveys a far broader scope of interpretive flexibility, particularly given that this term is at the core of the Commission's own organic statute, the FTC Act.

LabMD similarly invokes *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000), for the proposition that "simple 'common sense as to the manner in which Congress is likely to delegate a policy decision of such economic and political magnitude' . . . reinforces the conclusion that the FTC lacks the authority to regulate the acts or practices alleged in the Complaint." Motion at 19 (quoting *Brown & Williamson*, 529 U.S. at 133). But *Brown & Williamson* is inapposite as well. In that case, the Court found that the Food and Drug Administration's attempts to regulate tobacco products conflicted directly with concrete manifestations of congressional intent. In particular, the Court concluded that, if the FDA had the authority it claimed, its own findings would have compelled it to ban tobacco products outright, whereas various tobacco-related statutes made clear that Congress wished *not* to ban such products. *See* 529 U.S. at 137-39. Here, of course, LabMD can cite no similar congressional intent to preserve inadequate data security practices that unreasonably injure consumers.

Similarly, the Court found that "Congress' specific intent when it enacted the FDCA" (Food, Drug & Cosmetics Act) in 1938 was to deny the FDA authority to regulate tobacco products. 529 U.S. at 146. The Court reasoned that, "*given the economic and political significance of the tobacco industry at the time*, it is extremely unlikely that Congress could have intended to place tobacco within the ambit of the FDCA absent any discussion of the matter." *Id.* at 147 (emphasis added).[5] By contrast, when enacting the FTC Act in 1914 and amending it in 1938, Congress had no way of anticipating the "economic and political significance" of data security practices in today's online environment. Accordingly, the fact that "there is no evidence in the text of the [FTC Act] or its legislative history that Congress in 1938 even considered the applicability of the Act" to data security practices is completely irrelevant. Congress could not possibly have had any "specific intent" to deny the FTC authority over data security practices. It did, however, intend to delegate broad authority to the FTC to address emerging business practices – including those that were unforeseeable when the statute was enacted. That is the only congressional intent that matters here.

B. The Commission Has Consistently Affirmed Its Authority under the FTC Act to Take Enforcement Action against Unreasonable Data Security Activities that Qualify as Unfair Acts and Practices

LabMD similarly attempts to draw support from the *Brown & Williamson* Court's determination that the FDA's 1996 "assertion of authority to regulate tobacco products" contradicted the agency's previous "consistent and repeated statements [over the preceding 73 years] that it lacked authority . . . to regulate tobacco absent claims of therapeutic benefit by the manufacturer," and the Court's conclusion that congressional enactments "against the backdrop" of the FDA's historic disavowal of authority confirmed that Congress did not intend to authorize such regulation. 529 U.S. at 132, 144-46. LabMD argues, by analogy, that "the Commission

[5] As the D.C. Circuit has recently recognized, these considerations are essential to the holding of *Brown & Williamson*, and, in their absence, that case does not justify restricting agency action under a broad statutory mandate. *See Verizon v. FCC*, No. 11-1355, at 23-25 (D.C. Cir., Jan. 14, 2014) (slip op.).

[previously] did not claim Section 5 'unfairness' authority to regulate patient-information (or any other) data-security practices," but "recently reversed course without explanation," thus purportedly defying congressional intent. Motion at 16, 18.

That analogy, too, is without merit. Unlike the FDA, the Commission has never disavowed authority over online privacy or data security matters. To the contrary, "[t]he Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace," and has repeatedly and consistently affirmed its authority to challenge unreasonable data security measures as "unfair . . . acts or practices" in violation of Section 5. *See* FTC Report to Congress, *Privacy Online*, at 2 (June 1998) ("*1998 Online Privacy Report*").[6] LabMD cites out-of-context snippets from the Commission's 1998 and 2000 reports to Congress for the unfounded proposition that, at that time, the Commission believed its authority over data security matters was "limited to ensuring that Web sites follow their stated information practices."[7] LabMD's characterization does not withstand scrutiny. Neither the text it quotes nor the reports as a whole can plausibly be read as disavowing the Commission's authority to take enforcement action against data security practices that violate Section 5's prohibition of "unfair . . . acts or practices," as defined in Section 5(n). Indeed, the Commission clearly stated that certain conduct relating to online data security is "likely to be an unfair practice," and, in both reports, confirmed its view that the FTC Act "provides a basis for government enforcement" against information practices [that] may be inherently . . . unfair, regardless of whether the entity has publicly adopted any fair information practice policies."[8] In context, the sentences from the 1998 and 2000 reports relied upon by LabMD simply recognize that the Commission's existing authority may not be sufficient to effectively protect consumers with regard to *all* data privacy issues of potential concern (such as aspects of children's online privacy) and that expanded rulemaking authority and enforcement remedies could enhance the Commission's ability to meaningfully address a broader range of such concerns.[9] The same

---

[6] *See* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[7] Motion at 16 n.12 (quoting *1998 Online Privacy Report* at 41) ("As a general matter, the Commission lacks authority to require firms to adopt information practice policies."); Reply at 7-8 (quoting FTC Report to Congress, *Privacy Online: Fair Information Practices in the Electronic Age* (May 2000) ("*2000 Online Privacy Report*") (http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf) ("As a general matter, . . . the Commission lacks authority to require firms to adopt information practice policies or to abide by the fair information practice principles on their Web sites").

[8] *1998 Online Privacy Report* at 12-13, 40-41. *See also 2000 Online Privacy Report* at 33-34 ("The Commission's authority over the collection and dissemination of personal data collected online stems from Section 5[,]" which "prohibits unfair and deceptive practices in and affecting commerce," and thus "authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of the Act, and provides a basis for government enforcement of certain [norms concerning] fair information practices").

[9] *See 1998 Online Privacy Report* at 42 (recognizing that "Section 5 may only have application to some but not all practices that raise concern about the online collection and use of information from children," and recommending legislation authorizing the Commission to promulgate "standards of practice governing the online collection and use of information from children."); *2000 Online Privacy Report* at

error infects LabMD's mischaracterization of testimony that Commissioners and high-level Commission staff members delivered to various congressional committees and subcommittees.[10]

Since the late 1990s, the Commission has repeatedly affirmed its authority to take action against unreasonable data security measures as "unfair . . . acts or practices" in violation of Section 5, in reports, testimony to Congress, and other publicly-released documents.[11] The Commission has also confirmed this view by bringing administrative adjudicatory proceedings and cases in federal court challenging practices that compromised the security of consumers' data and resulted in improper disclosures of personal information collected from consumers online. For example, on May 1, 2006, the Commission filed a complaint in the U.S. District Court for the District of Wyoming, charging that defendant Accusearch, Inc. and its principal obtained consumers' private information (specifically, data concerning their telecommunications usage) and caused such data to be disclosed to unauthorized third parties without consumers' knowledge or consent. *FTC v. Accusearch, Inc.*, Case No. 2:06-cv-0105, Complaint, at ¶¶ 9-13. The Commission alleged that this conduct was "an unfair practice in violation of Section 5(a) of the FTC Act," *id.*, ¶ 14, because it "caused or [was] likely to cause substantial injury to consumers that [was] not reasonably avoidable by consumers and [was] not outweighed by

---

36-37 (seeking legislation granting "authority to promulgate more detailed standards pursuant to the Administrative Procedure Act," including "rules or regulations [that] could provide further guidance to Web sites by defining fair information practices with greater specificity[,]"such as "what constitutes 'reasonable access' and 'adequate security'"). *See also* Motion at 17 n.13 (quoting same).

[10] *See* Motion at 16-17, nn.12, 13, 14 (citing testimony by Chairman Robert Pitofsky in 1998, then-Commissioner Edith Ramirez in 2011, Chairman Jonathan Leibowitz in 2012, and Bureau Directors Eileen Harrington and David Vladeck in 2009 and 2011, respectively). In such testimony, the FTC representatives conveyed the Commission's support for draft data security legislation that would expand the FTC's *existing* authority by providing it with rulemaking authority under the Administrative Procedure Act and civil penalty authority. *See, e.g.*, Prepared Statement of the FTC, *Data Security*, presented by Commissioner Edith Ramirez to House Comm. on Energy & Commerce, Subcomm. on Commerce, Mfg., and Trade, at 11-12 (June 5, 2011) (http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf).

[11] *See, e.g.*, Prepared Statement of the FTC, *Identity Theft: Innovative Solutions for an Evolving Problem*, presented by Bureau Dir. Lydia B. Parnes to Senate Comm. on the Judiciary, Subcomm. on Terrorism, Tech., and Homeland Security, at 5-6 (Mar. 21, 2007) (http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-identity-theft-innovative-solutions-evolving-problem/p065409identitytheftsenate03212007.pdf); FTC Staff Report, *Protecting Consumers in the Next Tech-ade*, at 29-30 (Spring 2008) (http://www.ftc.gov/sites/default/files/documents/reports/protecting-consumers-next-tech-ade-report-staff-federal-trade-commission/p064101tech.pdf); FTC Report, *Security in Numbers, SSNs and ID Theft*, at 7 (Dec. 2008) (http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf); Prepared Statement of the FTC, *Protecting Social Security Numbers From Identity Theft*, presented by Assoc. Bureau Dir. Maneesha Mithal to House Comm. on Ways and Means, Subcomm. on Soc. Security, at 8 (April 13, 2011) (http://ftc.gov/os/testimony/110411ssn-idtheft.pdf); FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change*, at 14, 73 (March 26, 2012) (http://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers). *See also* note 13, *infra*.

countervailing benefits to consumers or competition." *Id.*, ¶ 13. The district court agreed, granting summary judgment to the Commission in 2007, and the Tenth Circuit affirmed in 2009. *See Accusearch*, *supra*, 570 F.3d 1187. Since then, the Commission has taken the same position in dozens of other enforcement proceedings, including administrative adjudications,[12] as well as complaints filed in federal courts, *see* CC Opp. at 12-13 n.9 (citing cases). In these cases, the Commission challenged allegedly unreasonable data security measures (or other practices that enabled unauthorized third parties to harm consumers by obtaining access to their confidential personal data) as "unfair acts or practices" in violation of Section 5. And in each case, it clearly reaffirmed its position that it possessed jurisdiction over the allegedly "unfair" data security practices under Section 5.

The fact that the Commission initially focused its enforcement efforts primarily on "deceptive" data security practices, and began pursuing "unfair" practices in 2005, does not mean that the Commission lacked jurisdiction over "unfair" practices before then. As then-Commissioner Orson Swindle testified to a House subcommittee in 2004, "To date, the Commission's security cases have been based on its authority to prevent deceptive practices," but it "also has authority to challenge practices as unfair if they cause consumers substantial injury that is neither reasonably avoidable nor offset by countervailing benefits. The Commission has used this authority in appropriate cases to challenge a variety of injurious practices, including unauthorized charges in connection with 'phishing.'"[13] LabMD cites Commissioner Swindle's reference to the Commission's "deceptiveness" authority over data security practices, *see* Motion at 16 n.12, but neglects to mention his reference to the Commission's "unfairness" authority over such practices.

LabMD also misinterprets the Commission's expressions of support for legislation relating to data security as requests for authority to fill regulatory "gaps" that it could not fill without such legislation. *Id.* at 17 & nn.13, 14. LabMD refers to three data security-related laws that the Commission supported, and that Congress ultimately enacted – *i.e.*, the GLB Act,[14] the

---

[12] *See BJ's Wholesale Club, Inc.*, 140 F.T.C. 465, 470 (2005); *DSW, Inc.*, 141 F.T.C. 117, 122 (2006); *CardSystems Solutions, Inc.*, Docket No. C-4168, 2006 WL 2709787, *3 (Sept. 5, 2006); *Reed Elsevier, Inc.*, Docket No. C-4226, 2008 WL 3150420, *4 (July 29, 2008); *TJX Cos., Inc.*, Docket No. C-4227, 2008 WL 3150421, *3 (Sept. 29, 2008). In these and similar cases, the Commission issues its final Decisions & Orders only after placing the relevant proposed consent orders on the public record, issuing Notices in the Federal Register that summarize and explain the provisions of the proposed orders and invite public comment, and considering comments filed by interested members of the public. *See* 16 C.F.R. § 2.34(c) & (e).

[13] Prepared Statement of the FTC, *Protecting Information Security and Preventing Identity Theft*, presented by Commissioner Orson Swindle to House Comm. on Gov't Reform, Subcomm. on Tech., Info. Policy, Intergovernmental Relations, and the Census, at 7, 14 n.24 (Sept. 22, 2004) (http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-protecting-information-security-and-preventing-identity/040922infosecidthefttest.pdf) ("*Comm'r Swindle's 2004 Information Security Testimony*").

[14] Pub. L. 106-102 (1999) (codified in pertinent part at 15 U.S.C. § 6804(a)(1)).

Children's Online Privacy Protection Act ("COPPA"),[15] and the Fair and Accurate Credit Transactions Act of 2003 ("FACTA").[16] But these laws *recognized* the Commission's *existing* enforcement authority, *expanded* that authority in particular respects, and affirmatively *directed* the Commission to take particular actions to protect consumer interests in specified contexts. For example, in COPPA, Congress authorized the Commission to sue for civil penalties in addition to the equitable monetary relief available under existing law, and authorized and directed the Commission to promulgate rules to protect children's online privacy pursuant to the streamlined procedures of the Administrative Procedure Act ("APA"), rather than using the more time-consuming procedures mandated by Section 18 of the FTC Act, 15 U.S.C. § 57a. Similarly, in both FACTA and the GLB Act, Congress directed the Commission to adopt rules addressing specified topics using streamlined APA procedures; and in FACTA, Congress also expanded the range of remedies available in Commission enforcement actions.

Finally, even if they were otherwise plausible, LabMD's arguments about the intended meaning of the past statements of the Commission or its members or staff would still be immaterial to the ultimate question of the Commission's statutory authority. "An agency's initial interpretation of a statute that it is charged with administering is not 'carved in stone,'" and agencies "must be given ample latitude to 'adapt their rules and policies to the demands of changing circumstances." *Brown & Williamson*, 529 U.S. at 156-57 (quoting *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 863 (1984); *Smiley v. Citibank (S.D.)*, 517 U.S. 735, 742 (1996); *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 42 (1983); and *Permian Basin Area Rate Cases*, 390 U.S. 747, 784 (1968)); *see also Verizon v. FCC*, *supra* note 5, at 19-20. Presented with the concrete circumstances of this case, the Commission concludes that it can and should address whether or not LabMD's data security procedures constitute "unfair . . . acts or practices" within the meaning of the FTC Act. To conclude otherwise would disregard Congress's instruction to the Commission to protect consumers from harmful practices in evolving technological and marketplace environments.

C. HIPAA and Other Statutes Do Not Shield LabMD from the Obligation to Refrain from Committing Unfair Data Security Practices that Violate the FTC Act.

Contrary to LabMD's contention, Congress has never enacted any legislation that, expressly or by implication, forecloses the Commission from challenging data security measures that it has reason to believe are "unfair . . . acts or practices." LabMD relies on numerous "targeted statutes" that Congress has enacted in recent years "specifically delegating" to the Commission or to other agencies "statutory authority over data-security" in certain narrower fields. Motion at 15. But LabMD has not identified a single provision in any of these statutes that expressly withdraws any authority from the Commission. Thus, its argument that these more specific statutes implicitly repeal the FTC's preexisting authority is unpersuasive. "The cardinal rule is that repeals by implication are not favored. Where there are two acts upon the same subject, effect should be given to both if possible." *Posadas v. Nat'l City Bank of N.Y.*,

[15] Pub. L. 105-277 (1998) (codified in pertinent part at 15 U.S.C. §§ 6502(b), 6505(d)).

[16] Pub. L. 108-159 (2003) (codified in pertinent part at 15 U.S.C. § 1681s(a)).

296 U.S. 497, 503 (1936). Thus, one cannot conclude that Congress implicitly repealed or narrowed the scope of an existing statute (*i.e.*, Section 5) by subsequently enacting a new law unless "the intention of the legislature to repeal [is] clear and manifest; otherwise, at least as a general thing, the later act is to be construed as a continuation of, and not a substitute for, the first act . . . ." *Id.*; *see also Branch v. Smith*, 538 U.S. 254, 273 (2003) ("An implied repeal will only be found where provisions in two statutes are in 'irreconcilable conflict,' or where the [later] Act covers the whole subject of the earlier one and 'is clearly intended as a substitute.'"); *Morton v. Moncari*, 417 U.S. 535, 551 (1974) ("when two statutes are capable of co-existence, it is the duty of the courts, absent a clearly expressed congressional intention to the contrary, to regard each as effective").

Nothing in HIPAA, HITECH,[17] or any of the other statutes LabMD cites reflects a "clear and manifest" intent of Congress to restrict the Commission's authority over allegedly "unfair" data security practices such as those at issue in this case. LabMD identifies no provision that creates a "clear repugnancy" with the FTC Act, nor any requirement in HIPAA or HITECH that is "clearly incompatible" with LabMD's obligations under Section 5. *See* Motion at 13. To the contrary, the patient-information protection requirements of HIPAA are largely consistent with the data security duties that the Commission has enforced pursuant to the FTC Act. Indeed, the FTC and the Department of Health and Human Services ("HHS") have worked together "to coordinate enforcement actions for violations that implicate both HIPAA and the FTC Act." HHS, *Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules*, Final Rule, 78 Fed. Reg. 5566, 5579 (Jan. 25, 2013). And the two agencies have obtained favorable results by jointly investigating the data security practices of companies that may have violated each of these statutes.[18]

LabMD further argues that HIPAA's comprehensive framework governing "patient-information data-security practices" by HIPAA-regulated entities somehow trumps the

---

[17] *See* Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. 104-191 (1996) (codified in pertinent part at 42 U.S.C. §§ 1320d *et seq.*); American Recovery and Reinvestment Act of 2009, Pub. L. 111-5, Div. A, Title XIII, and Div. B, Title IV ("Health Information Technology for Economic and Clinical Health Act") ("HITECH") (codified at 42 U.S.C. §§ 1320d-5 *et seq.*).

[18] For example, in 2009, CVS Caremark simultaneously settled HHS charges of HIPAA violations and FTC charges of FTC Act violations, stemming from the two agencies' coordinated investigations of the company's failure to securely dispose of documents containing consumers' sensitive financial and medical information. *See* FTC Press Release: *CVS Caremark Settles FTC Charges: Failed to Protect Medical and Financial Privacy of Customers and Employees; CVS Pharmacy Also Pays $2.25 Million to Settle Allegations of HIPAA Violations* (Feb. 18, 2009) (http://www.ftc.gov/news-events/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial); *CVS Caremark Corp.*, Consent Order, FTC Docket No. C-4259, 2009 WL 1892185 (June 18, 2009). *See also* HHS Press Release: *CVS Pays $2.25 Million and Toughens Practices to Settle HIPAA Privacy Case* (Feb. 18, 2009) (http://www.hhs.gov/news/press/2009pres/02/20090218a.html). Similarly, in 2010, Rite Aid entered consent decrees to settle both FTC charges of FTC Act violations and HHS charges of HIPAA violations, which the two agencies had jointly investigated. *See Rite Aid Corp.*, Consent Order, 150 F.T.C. 694 (2010); HHS Press Release: Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case (July 27, 2010) (http://www.hhs.gov/news/press/2010pres/07/20100727a.html).

application of the FTC Act to that category of practices. Motion at 11-12. But HIPAA evinces no congressional intent to preserve anyone's ability to engage in inadequate data security practices that unreasonably injure consumers in violation of the FTC Act, and enforcement of that Act thus fully comports with congressional intent under HIPAA. LabMD similarly contends that, by enacting HIPAA, Congress vested HHS with "exclusive administrative and enforcement authority with respect to HIPAA-covered entities under these laws." *Id.* at 11. That argument is also without merit. To be sure, the Commission cannot enforce HIPAA and does not seek to do so.[19] But nothing in HIPAA or in HHS's rules negates the Commission's authority to enforce the FTC Act.[20]

Indeed, the FTC Act makes clear that, when Congress wants to exempt a particular category of entities or activities from the Commission's authority, it knows how to do so explicitly – further undermining LabMD's claim to an implicit "carve-out" from the Commission's jurisdiction over HIPAA-covered entities or their "patient-information data security practices." Section 5(a)(2) specifically lists categories of businesses whose acts and practices are not subject to the Commission's authority under the FTC Act. These include banks, savings and loans, credit unions, common carriers subject to the Acts to regulate commerce, air carriers, and entities subject to certain provisions in the Packers and Stockyards Act of 1921. 15 U.S.C. § 45(a)(2). Congress could have added "HIPAA-covered entities" to that list, but it did not. Similarly, the statute identifies certain types of practices that the Commission may not address, such as commerce with foreign nations in certain circumstances. *Id.* § 45(a)(3). But it provides no carve-out for data security practices relating to patient information, to which HIPAA may apply.

LabMD relies on *Credit Suisse Securities, LLC v. Billing*, 551 U.S. 264 (2007), for the proposition that industry-specific requirements in other statutes may trump more general laws such as the FTC Act. *See* Motion at 13. *Credit Suisse* is clearly distinguishable. As LabMD concedes, there was a "possible conflict between the [securities and antitrust] laws," creating a "risk that the specific securities and general antitrust laws, if both applicable, would produce conflicting guidance, requirements, . . . or standards of conduct." *Id.* By contrast, nothing in the

[19] LabMD repeatedly – but incorrectly – asserts that "the FTC agrees that LabMD has not violated HIPAA or HITECH." *See, e.g.*, Motion at 13; *see also* Reply at 4 ("a company FTC admits *complied* with HIPAA/HITECH in all respects") (emphasis in original); *id.* at 5 ("FTC admits LabMD has always complied with all applicable data-security regulations"); *id.* at 12 ("FTC *admits* that LabMD, a HIPAA-covered entity, always complied with HIPAA/HITECH regulations") (emphasis in original). The Commission does not enforce HIPAA or HITECH, and has never expressed any view on whether LabMD has, or has not, violated those statutes.

[20] Both HHS (pursuant to HIPAA and HITECH) and the FTC (pursuant to the American Recovery and Reinvestment Act of 2009) have promulgated regulations establishing largely congruent requirements concerning notification of data breaches involving consumers' private health information, but they are applicable to two different categories of firms. *Compare* 16 C.F.R. Part 318 (FTC rule) *with* 45 C.F.R. Part 164, Subparts D & E (HHS rule). LabMD correctly notes that this FTC rule does not apply to HIPAA-covered entities, *see* Motion at 12 & n.9, but the conclusion it draws from this fact is unfounded. Significantly, the Complaint in the present proceeding alleges only statutory violations; it does not allege violations of the FTC's Health Breach Notification Rule.

FTC Act compels LabMD to engage in practices forbidden by HIPAA, or vice versa. It is not unusual for a party's conduct to be governed by more than one statute at the same time, as "we live in 'an age of overlapping and concurrent regulatory jurisdiction[.]'" *FTC v. Ken Roberts Co.*, 276 F.3d 583, 593 (D.C. Cir. 2001) (quoting *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192 (D.C. Cir. 1996)). LabMD and other companies may well be obligated to ensure their data security practices comply with both HIPAA and the FTC Act. But so long as the requirements of those statutes do not conflict with one another, a party cannot plausibly assert that, because it complies with one of these laws, it is free to violate the other. Indeed, courts have consistently ruled that "the FTC may proceed against unfair practices even if those practices [also] violate some other statute that the FTC lacks authority to administer." *Accusearch*, 570 F.3d at 1194-95 (concluding that conduct may be an unlawful "unfair . . . act or practice" under the FTC Act even if it also violates the Telecommunications Act of 1996). *See also Orkin Exterminating Co.*, 849 F.2d at 1353 (rejecting proposition that a "mere breach of contract . . . is outside the ambit of [the "unfairness" prohibition in] section 5"); *Am. Fin. Servs. Ass'n*, 767 F.2d at 982-83 (FTC may ban certain creditor remedies, such as wage assignments and repossession of consumers' household goods, as "unfair . . . acts or practices" under the FTC Act, even where such conduct also ran counter to state laws against enforcing unconscionable contracts of adhesion).

Finally, LabMD argues that Congress' enactment of three new statutes addressing the Commission's authority over certain data protection matters in discrete contexts implies that Congress must have believed that, in other respects, the Commission lacked statutory authority to address data protection matters under the FTC Act. That argument, too, is without merit. First, as discussed above, in each of these statutes Congress *expanded* the enforcement and rulemaking tools that the Commission *already* possessed for addressing data security problems in discrete areas. *See supra* at 8 n.10, 9-10. LabMD identifies nothing in any of those bills or their legislative histories indicating that the Commission's authority to enforce Section 5's prohibition of "unfair . . . acts or practices" was limited in any way. Moreover, these statutes affirmatively *directed* the Commission to take particular actions to protect consumer interests in specified contexts.[21] Of course, by *compelling* the Commission to take particular steps in those contexts, Congress did not somehow divest the Commission of its preexisting and much broader *authority* to protect consumers against "unfair" practices. Congress commonly authorizes agencies to oversee entire fields while specifying, in a few areas, what minimum steps those agencies must take in exercising that authority, and the enumeration of those minimum steps does not cast doubt on the agencies' broader authority. *See, e.g.*, *Cablevision Sys. Corp. v. FCC*, 649 F.3d 695, 705-06 (D.C. Cir. 2011). And LabMD's reliance on data security-related bills that ultimately were *not* enacted into law (*see* Motion at 17-18 & n.15; Reply at 9) contradicts basic principles of statutory interpretation.[22]

[21] For example, in COPPA, Congress directed the Commission to promulgate rules addressing the specific duties of child-directed website operators to provide specific notices and obtain parental consent before collecting or disclosing children's personal information. *See* 15 U.S.C. § 6502(b).

[22] The fact that a proposed bill was not enacted into law does not mean that Congress consciously "rejected" it. Enacting a bill into law is a notoriously difficult and time-consuming process, given the procedural and political hurdles to be overcome before obtaining majority votes of both Houses of Congress, reconciliation of any differences between the two Houses' versions, and signature by the President. Thus, "the fact that Congress has considered, but failed to enact, several bills" typically sheds

In sum, we reject LabMD's contention that the Commission lacks authority to apply the FTC Act's prohibition of "unfair . . . acts or practices" to data security practices, in the field of patient information or in other contexts; and we decline to dismiss the Complaint on that basis.

II. THE COMMISSION HAS AUTHORITY TO ENFORCE THE STATUTE BY ADJUDICATING ALLEGED VIOLATIONS, DESPITE THE ABSENCE OF REGULATIONS, WITHOUT INFRINGING LABMD'S DUE PROCESS RIGHTS.

A. Administrative Agencies May Interpret and Enforce Statutory Requirements in Case-by-Case Adjudications, as Well as By Rulemaking.

LabMD argues that the Commission may not adjudicate whether the alleged conduct violated Section 5 of the FTC Act because the Commission "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." Motion at 23. LabMD asserts that "[t]he FTC's refusal to issue regulations is wrongful and makes no sense." *Id.* at 24. LabMD's position conflicts with longstanding case law confirming that administrative agencies may – indeed, must – enforce statutes that Congress has directed them to implement, regardless whether they have issued regulations addressing the specific conduct at issue. Thus, in the leading case of *SEC v. Chenery*, the Supreme Court recognized that the SEC had not exercised its statutory rulemaking authority with regard to the matter at issue, and squarely rejected the contention "that the failure of the Commission to anticipate this problem and to promulgate a general rule withdrew all power from that agency to perform its statutory duty in this case." 332 U.S. 194, 201-02 (1947). To the contrary: "the Commission had a statutory duty to decide the issue at hand in light of the proper standards[,] and . . . this duty remained 'regardless of whether those standards previously had been spelled out in a general rule or regulation.'" *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 292 (1974) (quoting *Chenery*, 332 U.S. at 201).

The Commission has long recognized that "information security is an ongoing process of assessing risks and vulnerabilities: no one static standard can assure appropriate security, as security threats and technology constantly evolve." *See Comm'r Swindle's 2004 Information Security Testimony* at 3. Such complex questions relating to data security practices in an online environment are particularly well-suited to case-by-case development in administrative adjudications or enforcement proceedings, given the difficulty of drafting generally applicable regulations that fully anticipate the concerns that arise over emerging business arrangements in this rapidly changing area. As the Supreme Court has explained,

---

little, if any, light on what Congress believed or intended; and the adjudicator's "task . . . is not to construe bills that Congress has failed to enact, but to construe statutes that Congress has enacted." *Wright v. West*, 505 U.S. 277, 294 n.9 (1992) (Thomas, J.) (plurality op.); *see also Verizon v. FCC*, *supra* note 5, at 25 ("pieces of subsequent failed legislation tell us little if anything about the original meaning" of a statute, and thus such later, unenacted legislative proposals provide "an unreliable guide to legislative intent") (citations omitted).

> [P]roblems may arise . . . [that] must be solved despite the absence of a relevant general rule. Or the agency may not have had sufficient experience with a particular problem to warrant rigidifying its tentative judgment into a hard and fast rule. Or the problem may be so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule. In those situations, the agency must retain power to deal with the problems on a case-to-case basis if the administrative process is to be effective. There is thus a very definite place for the case-by-case evolution of statutory standards. And the choice made between proceeding by general rule or by individual, ad hoc litigation is one that lies primarily in the informed discretion of the administrative agency.

Chenery, 332 U.S. at 202-03. Accordingly, "agency discretion is at its peak in deciding such matters as whether to address an issue by rulemaking or adjudication[,] [and] [t]he Commission seems on especially solid ground in choosing an individualized process where important factors may vary radically from case to case." *American Gas Ass'n v. FERC*, 912 F.2d 1496, 1519 (D.C. Cir. 1990). *See also FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 384-85 (1965) ("the proscriptions [of unfair or deceptive acts and practices] in Section 5 are flexible, to be defined with particularity by the myriad of cases from the field of business," which "necessarily give[] the Commission an influential role in interpreting Section 5 and in *applying it to the facts of particular cases arising out of unprecedented situations*.") (emphasis added).

The Commission has enforced Section 5's prohibition of "unfair . . . acts or practices" primarily through case-by-case adjudication and litigation from the time the statute was enacted. Indeed, numerous recent cases have condemned conduct that facilitated identity theft or involved misuse of confidential consumer information as unlawful "unfair . . . acts or practices," although the practices were unprecedented and not covered by any preexisting rules. Thus, even though the Commission had never promulgated any regulations governing the creation of online checks or bank drafts without adequate verification procedures, the Ninth Circuit, in *Neovi*, easily affirmed both the district court's holding that the defendants had committed "unfair acts or practices," 604 F.3d at 1155-58, and its requirement that the defendants disgorge all revenue from the unlawful conduct. *Id.* at 1159-60. Similarly, despite the absence of any regulation prohibiting online data brokers from gathering and selling consumers' confidential information gleaned from telephone records, the Tenth Circuit affirmed a district court decision finding that the defendants' conduct constituted "unfair acts and practices" and imposing an equitable disgorgement remedy. *See generally Accusearch*, 570 F.3d 1187.

B. This Proceeding Respects LabMD's Due Process Rights

The Commission's decision to proceed through adjudication without first conducting a rulemaking also does not violate LabMD's constitutional due process rights. The courts have rejected such due process challenges to agency adjudications on numerous occasions. For example, in *Gonzalez v. Reno*, 212 F.3d 1338 (11th Cir. 2000), the court held that the agency did not violate due process in interpreting and implementing the immigration statute in an

enforcement proceeding, even though its "policy was developed in the course of an informal adjudication, rather than during formal rulemaking." 212 F.3d at 1350. *See also Taylor v. Huerta*, 723 F.3d 210, 215 (D.C. Cir. 2013) (statute enabling agency to revoke pilot's license following administrative adjudicatory proceeding "represented nothing more than an ordinary exercise of Congress' power to decide the proper division of regulatory, enforcement, and adjudicatory functions between agencies in a split-enforcement regime . . . . [Petitioner] cites no authority, and presents no persuasive rationale, to support his claim that due process requires more."); *RTC Transp., Inc. v. ICC*, 731 F.2d 1502, 1505 (11th Cir. 1984) (rejecting contention that agency's "application of its policy . . . denied them due process because the policy was announced in adjudicatory proceedings, . . . rather than being promulgated in rulemaking proceedings with notice and opportunity for comment"); *Shell Oil Co. v. FERC*, 707 F.2d 230, 235-36 (5th Cir. 1983) (noting that parties in administrative adjudicatory proceedings are not denied due process even when agencies establish new, binding standards of general application in such proceedings, so long as affected parties are given meaningful opportunities to address the factual predicates for imposing liability).

To be sure, constitutional due process concerns may arise if the government imposes criminal punishment or civil penalties for past conduct (or unduly restricts expression protected by the First Amendment) pursuant to a law that "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012) (quoting *United States v. Williams*, 553 U.S. 285, 304 (2008)). But, as the D.C. Circuit held in rejecting a constitutional due process challenge to the Commission's implementation of the Fair Credit Reporting Act,

> [E]conomic regulation is subject to a less strict vagueness test because its subject matter is often more narrow, and because businesses, which face economic demands to plan behavior carefully, can be expected to consult relevant legislation in advance of action. The regulated enterprise . . . may have the ability to clarify the meaning of the regulation by its own inquiry, or by resort to an administrative process. Finally, the consequences of imprecision are qualitatively less severe when laws have . . . civil rather than criminal penalties.

Trans Union Corp. v. FTC, 245 F.3d 809, 817 (D.C. Cir. 2001) (quoting *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498-99 (1982)).

Here, the three-part statutory standard governing whether an act or practice is "unfair," set forth in Section 5(n), should dispel LabMD's concern about whether the statutory prohibition of "unfair . . . acts or practices" is sufficient to give fair notice of what conduct is prohibited. In enacting Section 5(n), Congress endorsed the Commission's conclusion that "the unfairness standard is the result of an evolutionary process . . . . [that] must be arrived at by . . . a gradual process of judicial inclusion and exclusion." *Policy Statement on Unfairness*, 104 F.T.C. at 1072. This is analogous to the manner in which courts in our common-law system routinely develop or refine the rules of tort or contract law when applying established precedents to new

factual situations. As the Supreme Court has recognized, "[b]roadly worded constitutional and statutory provisions necessarily have been given concrete meaning and application by a process of case-by-case judicial decision in the common-law tradition." *Northwest Airlines, Inc. v. Transp. Workers Union of Am.*, 451 U.S. 77, 95 (1981).

LabMD's due process claim is particularly untenable when viewed against the backdrop of the common law of negligence. Every day, courts and juries subject companies to tort liability for violating uncodified standards of care, and the contexts in which they make those fact-specific judgments are as varied and fast-changing as the world of commerce and technology itself. The imposition of such tort liability under the common law of 50 states raises the same types of "predictability" issues that LabMD raises here in connection with the imposition of liability under the standards set forth in Section 5(n) of the FTC Act. In addition, when factfinders in the tort context find that corporate defendants have violated an unwritten rule of conduct, they – unlike the FTC – can normally impose compensatory and even punitive damages. Even so, it is well-established that the common law of negligence does not violate due process simply because the standards of care are uncodified. There is similarly no basis to conclude that the FTC's application of the Section 5(n) cost-benefit analysis violates due process, particularly where, as here, the complaint does not even seek to impose damages, let alone retrospective penalties.

III. LABMD'S ALLEGED PRACTICES ARE "IN OR AFFECTING COMMERCE" UNDER THE FTC ACT

In Section III of the Motion to Dismiss, LabMD contends that the acts and practices alleged in the Complaint do not satisfy the statutory definition of "commerce" set forth in Section 4 of the FTC Act – *i.e.*, "commerce 'among' or 'between' states." *See* Motion at 28 (citing and paraphrasing 15 U.S.C. § 44, and asserting that LabMD's principal place of business is in Georgia; the alleged acts or practices were committed in Georgia; and its servers and computer network are located in Georgia). This argument is frivolous. The Complaint plainly alleges that LabMD "tests samples from consumers located throughout the United States." Complaint, ¶ 5; *see also* ¶ 2. Indeed, LabMD concedes in its Answer to the Complaint that it "tests samples . . . which may be sent from six states outside of Georgia: Alabama, Mississippi, Florida, Missouri, Louisiana, and Arizona." Answer, ¶ 5. Thus, the complaint unquestionably alleges that LabMD's acts and practices "have been in or affecting commerce, as 'commerce' is defined in Section 4[.]" Complaint, ¶ 2.

IV. THE ALLEGATIONS IN THE COMPLAINT STATE A PLAUSIBLE CLAIM THAT LABMD ENGAGED IN "UNFAIR . . . ACTS OR PRACTICES"

We turn next to LabMD's contention that "the Complaint does not state a plausible claim for relief" on the ground that the "Complaint's allegations are nothing more than inadequate 'legal conclusions couched as factual allegations.'" Motion at 28-29 (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 554, 555 (2007)).

That is incorrect. The Complaint quite clearly sets forth specific allegations concerning LabMD's conduct and other elements of the charged violation. In particular, it includes plausible

allegations that satisfy each element of the statutory standard for unfairness: that (1) the alleged conduct caused, or was likely to cause, substantial injury to consumers; (2) such injury could not reasonably have been avoided by consumers themselves; and (3) such injury was not outweighed by benefits to consumers or competition. 15 U.S.C. § 45(n). We emphasize that, for purposes of addressing LabMD's Motion to Dismiss, we presume – without deciding – that these allegations are true. But the Commission's ultimate decision on LabMD's liability will depend on the factual evidence to be adduced in this administrative proceeding.

A. Causation or Likely Causation of Substantial Injury to Consumers

The Complaint contains sufficient allegations to satisfy the criterion that the respondent's acts or practices "cause[d], or [were] likely to cause, substantial injury to consumers." *Id.* First, the Complaint alleges that LabMD collected and stored on its computer system highly sensitive information on consumers' identities (*e.g.*, names linked with addresses, dates of birth, Social Security numbers, and other information), their medical diagnoses and health status, and their financial transactions with banks, insurance companies, and health care providers. *See* Complaint, ¶¶ 6-9, 19, 21.

Second, the Complaint contains allegations that LabMD implemented unreasonable data security measures. These measures allegedly included (*i*) "acts of commission," such as installing Limewire, a peer-to-peer file sharing application, on a billing manager's computer, *see id.*, ¶¶ 13-19, as well as (*ii*) "acts of omission," such as failing to institute any of a range of readily-available safeguards that could have helped prevent data breaches. *See id.*, ¶¶ 10(a)-(g)).

Third, the Complaint alleges that LabMD's actions and failures to act, collectively, directly caused "substantial injury" resulting from both (*i*) actual data breaches, enabling unauthorized persons to obtain sensitive consumer information, *id.*, ¶¶ 17-21, as well as (*ii*) increased risks of other potential breaches. *Id.*, ¶¶ 11-12, 22. Notably, the Complaint's allegations that LabMD's data security failures led to *actual* security breaches, if proven, would lend support to the claim that the firm's data security procedures caused, or were likely to cause, harms to consumers – but the mere fact that such breaches occurred, standing alone, would not necessarily establish that LabMD engaged in "unfair . . . acts or practices." The Commission has long recognized that "the occurrence of a breach does not necessarily show that a company failed to have reasonable security measures. There is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution." *See Comm'r Swindle's 2004 Information Security Testimony* at 4.[23] Accordingly, we will need to determine whether the "substantial injury" element is satisfied by considering not only whether the facts alleged in the Complaint actually occurred, but also whether LabMD's data security procedures

[23] *See also In re SettlementOne Credit Corp.*, File No. 082 3209, Letter to Stuart K. Pratt, Consumer Data Industry Association, from Donald S. Clark, Secretary, by Direction of the Commission, at 2 (Aug. 17, 2011) (http://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819lettercdia_1.pdf) (affirming, in resolving three cases concerning data security practices alleged to violate the Fair Credit Reporting Act, that it had "applied the standard that is consistent with its other data security cases – that of reasonable security. This reasonableness standard is flexible and recognizes that there is no such thing as perfect security.")

were "unreasonable" in light of the circumstances. Whether LabMD's security practices were unreasonable is a factual question that can be addressed only on the basis of evidence to be adduced in this proceeding.

Fourth, the Complaint alleges that the actual and potential data breaches it attributes to LabMD's data security practices caused or were likely to cause cognizable, "substantial injury" to consumers, including increased risks of "identity theft, medical identity theft," and "disclosure of sensitive private medical information." *See* Complaint, ¶ 12; *see also id.*, ¶¶ 11, 21-22. These allegations clearly refute LabMD's contentions that the Complaint contains "no allegations of monetary loss or other actual harm" nor "any actual, completed economic harms or threats to health or safety." Motion at 28-29. Moreover, occurrences of actual data security breaches or "actual, completed economic harms" (*id.* at 29) are not necessary to substantiate that the firm's data security activities caused or likely caused consumer injury, and thus constituted "unfair . . . acts or practices." *Accord Policy Statement on Unfairness*, 104 F.T.C. at 949 n.12 (act or practice may cause "substantial injury" if it causes a "small harm to a large number of people" or "raises a significant *risk* of concrete harm") (emphasis added); *accord Neovi*, 604 F.3d at 1157 (quoting *Am. Fin. Servs.*, 767 F.2d at 972).

B. Avoidability

The Complaint contains plausible allegations that these harms could not reasonably be avoided by consumers. Consumers allegedly did not have any "way of independently knowing about respondent's security failures," let alone taking any action to remedy them or avoid the resulting harm. Complaint, ¶ 12.

C. Countervailing Benefits to Consumers or Competition

Finally, the Complaint alleges that the alleged conduct did not even benefit LabMD, much less anyone else (*id.*, ¶ 20), and that LabMD could have remedied the risks of data breaches "at relatively low cost" (*id.*, ¶ 11). These allegations provide a plausible basis for finding that the harms to consumers were not outweighed by other benefits to consumers or competition. Again, Complaint Counsel will need to prove these allegations, and LabMD will have the opportunity to refute them, on the basis of factual evidence presented at the upcoming hearing.

* * * * *

For the reasons discussed above, we deny LabMD's Motion to Dismiss.

Accordingly,

IT IS ORDERED THAT Respondent LabMD, Inc.'s Motion to Dismiss Complaint with Prejudice **IS DENIED.**

By the Commission, Commissioner Brill recused.

Donald S. Clark
Secretary

SEAL:
ISSUED: January 16, 2014

EXHIBIT 3

January 21, 2014

Via CM/ECF

The Honorable Esther Salas
United States District Court
District of New Jersey
50 Walnut Street
Newark, NJ 07101

Re: *FTC v. Wyndham Worldwide Corp., et al.*, No. 2:13-cv-01887-ES-JAD

Dear Judge Salas:

Pursuant to the Court's order of December 27, 2013, the parties in the above-captioned matter respectfully submit the following supplemental letter brief.

I. Defendants' Position

A. The FTC Lacks Statutory Authority

The FTC, like any other federal agency, must show that Congress intended to delegate to it the specific authority it claims. *See La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374-75 (1986). The FTC has not done that. Nothing in Section 5 of the FTC Act gives the Commission all-encompassing authority to regulate the data-security practices of every company in America. And, by its own admission, the FTC cannot claim that authority by virtue of Congress's supposed acquiescence in the Commission's actions to date. *See* Mot. to Dismiss Oral Arg. Tr. ("Tr.") at 48:20-22 ("As [Defendants] pointed out in the reply brief, there is little point [in] trying to read tea leaves of Congressional inaction.").

Indeed, far from giving the FTC unfettered authority to regulate data-security in ***every*** sector of the economy, Congress has carefully circumscribed the FTC's data-security powers to certain narrow, well-defined subject matters. *See* Fair Credit Reporting Act ("FCRA"), Pub. L. 91-508, codified as amended at 15 U.S.C. § 1681 *et seq*. (consumer reporting agencies); Gramm-Leach-Bliley Act ("GLBA"), Pub. L. 106-102 (financial institutions); Children's Online Privacy Protection Act ("COPPA"), Pub. L. 105-277 (websites collecting information from children). Those targeted grants of authority would make no sense if Section 5 already gave the FTC authority to regulate data security in ***all*** circumstances. *See Duncan v. Walker*, 533 U.S. 167, 174 (2001) (explaining that statutes must be interpreted to avoid surplusage and "to give effect, if possible, to every clause and word"). Instead, the much more natural interpretation of Congressional intent is that Congress understood the FTC to possess no data-security powers at all, unless and until Congress enacted the FCRA, GLBA, and COPPA.

Faced with the plain conflict between its broad interpretation of Section 5 and the narrow grants of data-security authority that Congress has actually given the Commission, the FTC argues that Congress enacted the FCRA, GLBA, and COPPA merely to supplement the FTC's

existing general police power over data-security matters. That is revisionist history. Nothing in the text or legislative history of the FCRA, GLBA, or COPPA suggests that Congress has ever understood Section 5 of the FTC Act to give the FTC general police power to regulate data-security practices, and the FTC's attempts to argue otherwise are *post hoc* rationalizations intended to create out of whole cloth a statutory basis for the FTC's actions.

The FTC initially tried to square the FCRA, GLBA, and COPPA with the Commission's broad interpretation of Section 5 on the grounds that Congress enacted those statutes merely to grant the FTC "rulemaking and/or civil penalty authority" in certain specific contexts. *See* FTC Opp'n to WHR Mot. to Dismiss ("FTC Opp'n"), ECF No. 110, at 12. But far from being limited statutes that merely add civil-penalty and rulemaking authority to Section 5, the FCRA, GLBA, and COPPA each contain detailed provisions granting the FTC ***substantive*** authority over data-security practices, *see* 15 U.S.C. §§ 1681m(e)(1), 6804(a)(1)(C), 6502(b), and explicit authority to ***enforce*** those standards in limited contexts, *see id.* §§ 1681s(a), 6805(a)(7), 6505(d). The FCRA, for instance, directs the FTC to "prescribe regulations requiring [financial institutions] to establish reasonable policies and procedures . . . to identify possible risks to account holders." *Id.* § 1681m(e)(1)(B). And the GLBA instructs the FTC to "establish appropriate standards for the financial institutions subject to [its] jurisdiction relating to administrative, technical, and physical safeguards to insure the security and confidentiality of customer records and information." *Id.* § 6801(b). Those substantive grants of authority would have been entirely unnecessary if, as the FTC claims, the FCRA, GLBA, and COPPA did no more than merely add "rulemaking and/or civil penalty" powers to the FTC's existing Section 5 authority. FTC Opp'n at 12. The far more plausible interpretation is that Congress saw those substantive-authority provisions as necessary to give the FTC any authority at all over data-security matters, fundamentally undermining the FTC's belief that Section 5 already provided it that authority. *See, e.g.*, *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992) ("We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there."); *United States v. Ryan*, 350 U.S. 299, 305 (1956) ("If Congress intended to deal with that problem alone, it could have done so directly.").

For the first time at oral argument, the FTC advanced a second theory of how to reconcile the FCRA, GLBA, and COPPA with the Commission's novel interpretation of Section 5. According to the FTC, Congress always understood Section 5 to provide the FTC with general police power over data-security matters, but it enacted the FCRA, GLBA, and COPPA for the limited purpose of freeing the Commission from the need to prove substantial consumer injury in specific contexts. *See* Tr. at 45:8-12 ("[T]here is no injury requirement in those cases [under the FCRA, GLBA, and COPPA], so they are dramatically different than the FTC's authority under the FTC Act. Under the FTC Act we are limited to cases where we can prove substantial [in]jury.").

That is a far-fetched reconstruction of what Congress intended to accomplish in the FCRA, GLBA, and COPPA. The text of those statutes, to begin, does not support the FTC's understanding. If Congress really had intended to do no more than simply eliminate the substantial-consumer-injury requirement of Section 5, the data-security provisions of the FCRA, GLBA, and COPPA would have said little more than: "In enforcing Section 5 of the FTC Act in these circumstances, the FTC need not prove substantial injury to consumers." Needless to say, such language cannot be found in the text of these sector-specific statutes. To the contrary, the

FCRA, GLBA, and COPPA all contain detailed provisions granting the FTC ***substantive*** authority over data-security practices, something that would have been entirely unnecessary for Congress to do under the FTC's reconstruction of Congressional intent.

The context and legislative history of the FCRA, GLBA, and COPPA further undermine the FTC's argument that those sector-specific statutes were enacted merely to free the Commission from Section 5's consumer-injury requirement and not to provide the FTC with substantive authority it otherwise lacked. The legislative record shows that each statute was enacted in response to Congressional concerns over the collection and misuse of sensitive consumer data. *See, e.g.*, 149 Cong. Rec. H12198, H12214-15 (daily ed. Nov. 21, 2003) (conference report on the 2003 amendments to the FCRA, which granted the FTC data-security authority over the disposal of consumer credit information); H.R. Rep. 106-74(III) at 117-19 (1999) (committee report on the GLBA); 144 Cong. Rec. S8482, S8482-83 (daily ed. July 17, 1998) (statement of Sen. Bryan, drafter and co-sponsor of COPPA). Congress therefore enacted the FCRA, GLBA, and COPPA precisely because it believed that data security ***was not covered by existing statutory provisions***, including Section 5 of the FTC Act. Nothing in the legislative history supports the FTC's alternative theory that Congress already understood the FTC to have universal data-security authority under Section 5, but felt it necessary to enact three statutes to eliminate the consumer-injury requirement in certain circumstances.

Indeed, it is far from clear whether the FCRA, GLBA, and COPPA actually ***do*** eliminate the substantial-injury requirement in the first place. The FCRA and COPPA direct the FTC to enforce those statutes as though they included "***all applicable terms and provisions*** of the [FTC] Act." 15 U.S.C. § 6505(d) (emphasis added); *accord id.* § 1681s(a)(1) (directing the FTC to pursue violations of the FCRA and its underlying regulations "as though the applicable terms and conditions of the [FTC] Act were part of [the FCRA]"). That necessarily means the FTC must prove substantial, unavoidable consumer injury as a part of enforcing those statutes.* And although the statutes do alter ***some*** of the background requirements of the FTC Act, *see, e.g.*, § 1681s(a)(1), no provision of the FCRA, GLBA, or COPPA purports to relieve the FTC of its duty to prove substantial consumer injury. As a result, the FTC's asserted distinction between its sweeping understanding of Section 5 and the narrow delegations of the FCRA, GLBA, and COPPA is really not distinction at all—because both sets of statutes require substantial consumer injury, the FTC's understanding of Section 5 cannot be sustained without rendering the terms of the FCRA, GLBA, and COPPA entirely superfluous.

Finally, legislation recently proposed in Congress by Senator Patrick Leahy further confirms that the FTC lacks generalized data-security authority under Section 5. *See* Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. §§ 201-04. That legislation would require businesses with access to data on 10,000 or more individuals to establish "administrative, technical, or physical safeguards identified by the Federal Trade Commission." *Id.* § 202. The bill would also grant the FTC explicit enforcement authority over the data-security requirements

* The provisions in the FCRA, COPPA and GLBA providing that a violation of a regulation thereunder constitutes a violation of the FTC Act do nothing to alter this conclusion. See 15 U.S.C. § 1681s(a) (FCRA); *id*. §§ 6801(b), 6805(a)(7) (GLBA); *id*. § 6505(d) (COPPA). Rather than eliminating the substantial consumer injury requirement, those provisions implicitly acknowledge that these sector-specific statutes (and regulations validly enacted thereunder) already incorporate that requirement.

established thereunder. *See id.* § 203(b) ("Any business entity shall have the provisions of this subtitle enforced against it by the Federal Trade Commission."). Again, if the Commission already possessed plenary data security authority under Section 5, such comprehensive legislation would be unnecessary.

B. The FTC Has Not Provided Fair Notice

In any event, even if the FTC were correct in its understanding of the relevant statutes, its amended complaint should still be dismissed because the FTC has not provided regulated entities with the fair notice that the Due Process Clause requires. The FTC has not published any rules, regulations, or guidelines explaining to businesses what data-security protections they must employ to comply with the FTC's interpretation of Section 5 of the FTC Act. Such a failure to publish any interpretive guidance whatsoever violates the "fundamental principle in our legal system" that "laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." FCC v. Fox Television Stations, Inc., 132 S. Ct. 2307, 2317 (2012). It also violates bedrock principles of administrative law, which make clear that when a statute such as Section 5 is "so vague that [its] ambiguity can only be resolved by deferring to the agency's own interpretation," the agency must at the very least state with "ascertainable certainty" what conduct is prohibited. Sec. of Labor v. Beverly Healthcare-Hillview, 541 F.3d 193, 202 (3d Cir. 2008).

The FTC's lack of guidance has not gone unnoticed. Congress has expressed concern over "the regulatory uncertainty many businesses feel already" because the FTC has failed to provide "a coherent statement of policy on how the Commission plans to enforce Section 5." See Hearing on FTC Review and Outlook before the Subcomm. on Commerce, Manuf. and Trade of the House Comm. on Energy and Commerce, 113th Cong., 2013 WL 6237638 at 3 (Dec. 3, 2013). Without such a "coherent statement," one member noted, "many businesses, large and small, are left to examining past decisions to see how they may fit into a certain set of facts." Id. Similarly, leading business organizations participating in this case have explained that current FTC enforcement practices give "no advance notice to businesses on what they are required to do to comply with the law in a rapidly changing technological environment." Br. of Amici Curiae Chamber of Commerce of the United States, et al. at 11.

Nor would it be particularly difficult for the FTC to promulgate the rules and regulations that due process requires. Although the FTC has previously claimed that it would be "impossible" to craft generalized data-security rules, at least two other federal agencies have managed to do just that—and both of those agencies did so for computer networks much more sophisticated than those involved in this litigation. See Department of Homeland Security ("DHS") Office of Inspector General, Evaluation of DHS' Information Security Program for Fiscal Year 2013 (Nov. 21, 2013), available at http://goo.gl/OC4CNx [hereinafter, "DHS Evaluation"]; National Institute of Standards and Technology ("NIST") Preliminary Cybersecurity Framework: Improving Critical Infrastructure Cybersecurity (Oct. 22, 2013), available at http://goo.gl/ivPLnq [hereinafter, "NIST Framework"]. NIST recently released for public comment a 44-page document explaining precisely what data-security protocols should be employed to protect computer networks at "critical infrastructure" locations, including facilities such as nuclear power plants. See NIST Framework at 13-27. And DHS has, since at least 2008,

assessed the state of its own internal data security using an "Information Security Scorecard" with a 0-100 rating on various, specific data-security metrics. See, e.g., DHS Evaluation at 42.

If NIST and DHS are readily able to compile a set of objective data-security standards for critical infrastructure and homeland security applications, the FTC can certainly do the same for consumer payment applications in order to satisfy constitutional fair notice requirements. Although the FTC claims it has not engaged in rulemaking because of the difficulty in crafting standards that would apply to businesses of all types and sizes, see Tr. at 77:6-9, 18-23, that variation among regulated entities is precisely why Congress and the courts require rulemaking in these types of situations—to ensure that the agency considers the views of all stakeholders and then fashions a policy or rule that remedies the problem at issue in a sensible manner, see, e.g., Hall v. EPA, 273 F.3d 1146, 1163 (9th Cir. 2001) ("[T]he point of notice-and-comment rulemaking is that public comment will be considered by an agency and the agency may alter its action in light of those comments."). The FTC's concession that different standards should apply to different businesses confirms the arbitrary nature of its current approach, which leaves businesses guessing as to what they must do to avoid running afoul of the Commission's ad hoc data security policy.

Although it concedes that it has published no rules or regulations on data-security requirements, Tr. at 69:24-70:2, the FTC argues that its prior consent decrees and an informal brochure provide all the notice that due process mandates. FTC Opp'n at 18-20. But it is well-established that third-party agency consent decrees do not constrain FTC discretion and thus cannot provide any meaningful notice to third parties. See, e.g., United States v. E.I. du Pont de Nemours & Co., 366 U.S. 316, 330 n.12 (1961); Integraph Corp. v. Intel Corp., 253 F.3d 695, 698 (Fed. Cir. 2001) ("[A] consent order does not establish illegal conduct."). And the informal brochure on which the FTC so heavily relies, see FTC Opp'n at 18-19 (citing Protecting Personal Information: A Guide for Business (2007)), is far too vague to provide meaningful guidance, particularly in the complex world of data security. For proof of that, one need look no further than the 44 pages of guidance that NIST has propounded on the same subject, much of which contains references to other, even more detailed protocols. See NIST Framework at 13-27.

For these reasons, Defendants' motions to dismiss should granted. Defendants also request leave from this Court to file a two-page reply letter after the FTC has set out its arguments below. Because the FTC raised its substantial-injury argument for the first time at oral argument, the response below is the first time Defendants will have been provided with a written articulation of the FTC's position on these issues. Defendants therefore request that the Court grant Defendants leave to file a short reply brief, so that Defendants can respond properly to the FTC's arguments.

II. Plaintiff's Position

Section 5 of the FTC Act applies by its terms to *all* unfair commercial practices that violate the three-part statutory test of 15 U.S.C. § 45(n). The plain language of Section 5 is not susceptible to a "data security" exception. Wyndham thus resorts to an argument that Section 5 must not mean what it says because, if that plain-language interpretation were correct, Congress would not have needed to enact various subsequent statutes. *See supra* p. 2. That argument is wrong because, in at least three different respects, these statutes supplement the Commission's preexisting Section 5 authority. First, as discussed below, these statutes dispense with the "consumer injury" requirement that the FTC would otherwise face in any case it brings under Section 5. Second, these newer statutes grant the FTC additional powers, such as streamlined Administrative Procedure Act rulemaking authority and civil-penalty authority, each of which the FTC would otherwise lack. *See* Pl.'s Resp. in Opp'n to Mot. to Dismiss 12, ECF No. 110 ("Pl.'s Opp'n). Third, unlike the FTC Act itself, these newer statutes affirmatively compel (rather than merely authorize) the FTC to use its consumer-protection authority in specified ways. Those many differences alone undermine Wyndham's argument that, by enacting these statutes, Congress meant to carve out an atextual "data security" exception to the Commission's Section 5 authority.

We discuss the merits of these issues below, but we first note that any doubt about the FTC's statutory authority would be dispelled by two recent developments: (1) the FTC's recent decision in *LabMD*, which is entitled to full *Chevron* deference under *City of Arlington, Tex. v. FCC*, 133 S. Ct. 1863, 1871 (2013); and (2) the D.C. Circuit's decision in *Verizon v. FCC*, No. 11-1355, 2014 WL 113946, at *11-12 (D.C. Cir. Jan. 14, 2014), which rejects a very similar argument based on *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000).

The FTC's *LabMD* order. On January 16, 2014, the Federal Trade Commission entered an order in an administratively-pending Section 5 data security case against LabMD, in which the Commission addressed many of the arguments Wyndham makes in its Motions to Dismiss. *See LabMD, Inc.*, Order Den. Resp't Mot. to Dismiss 3-14, Docket No. 9357 (F.T.C. Jan. 16, 2014), ECF No. 151-1 ("LabMD Order"). In particular, in *LabMD*, the Commission explicitly, and thoroughly, rejected an identical statutory-authority argument, removing any doubt that Section 5 authorizes the FTC to enforce unfairness in the data security context. As the Supreme Court recently confirmed, under *Chevron*, courts "must defer to an agency's interpretation of statutory ambiguity that concerns the scope of the agency's statutory authority (that is, its jurisdiction)." *City of Arlington, Tex. v. FCC*, 133 S. Ct. 1863, 1868 (2013) (citing *Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837 (1984)). *See also Nat'l Cable & Telecomms Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 985 (2005) ("Before a judicial construction of a statute . . . may trump an agency's, the court must hold that the statute unambiguously requires the court's construction.").

The D.C. Circuit's Verizon decision. Wyndham's reliance on *Brown & Williamson* is untenable. *See* Pl.'s Opp'n 10-15; Mot. to Dismiss Hr'g Tr. 15-16, 45-46, ECF No. 139. The D.C. Circuit recently confirmed that point by rejecting a similar argument based on that decision for reasons that are instructive here. As the circuit court explained, the Supreme Court's

decision in *Brown & Williamson* turned on the fact "that the FDA had not only completely disclaimed any authority to regulate tobacco products, but had done so *for more than eighty years*." *Verizon*, 2014 WL 113946, at *11. Here, as previously explained, the FTC has never disclaimed its authority to enforce Section 5 unfairness in the data security context. *See* Pl.'s Opp'n 13-15, Mot. to Dismiss Hr'g Tr. 27-29; *accord* LabMD Order 7-10. Moreover, as the D.C. Circuit noted, the *Brown & Williamson* court deemed it significant "that the FDA's newly adopted conclusion that it did in fact have authority to regulate this industry would, given its findings regarding the effects of tobacco products and its authorizing statute, *logically require the agency to ban such products altogether, a result clearly contrary to congressional policy*." *Verizon*, 2014 WL 113946, at *11 (emphasis added). Like LabMD, Wyndham "can cite no similar congressional intent to preserve inadequate data security practices that unreasonably injure consumers." LabMD Order 6. Finally, none of the complementary statutes cited by Defendants conflict with the FTC's background Section 5 unfairness authority, let alone "logically require . . . a result clearly contrary to congressional policy." *Verizon,* 2014 WL 113946, at *11.

A. The FTC Act and Complementary Statutes

The Court specifically asked for supplemental briefing concerning the relationship between the FTC Act's injury requirement set forth in 15 U.S.C. § 45(n), and three other statutes the FTC enforces, all of which have data security components: the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681, *et seq*. (1970, amended 2003, 2010), the Gramm-Leach-Bliley Financial Modernization Act ("GLBA"), 15 U.S.C. § 6801, *et seq*. (1999), and the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501, *et seq*. (1998).

Section 45(n) limits the definition of "unfair acts or practices" under the FTC Act to those which "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." 15 U.S.C. § 45(n). For the FCRA, GLBA, and COPPA, Congress has in essence said that a violation of the terms of these statutes is itself a sufficient injury to permit the FTC to enforce the statute in federal court. "The passage of [a] statute is, in a sense, an implied finding that violations will harm the public and ought, if necessary, be restrained." *United States v. Diapulse Corp. of Am.*, 457 F.2d 25, 28 (2d Cir. 1972). *See also United States v. Cappetto*, 502 F.2d 1351, 1358-59 (7th Cir. 1974). For example, Congress has determined that when a credit reporting agency violates the FCRA by furnishing a consumer's financial data without a permissible purpose, that violation causes consumer injury. *See Trans Union Corp. v. FTC*, 267 F.3d 1138, 1142 (D.C. Cir. 2001) (*"Trans Union I"*) ("[T]he government cannot promote its interest (protection of personal financial data) except by regulating speech because the speech itself (dissemination of financial data) causes the very harm the government seeks to prevent."). *See also Trans Union LLC v. FTC*, 295 F.3d 42, 53 (D.C. Cir. 2002) (*"Trans Union II"*) (as in *Trans Union I*, in the GLBA context, the dissemination of financial data causes the very harm the government seeks to prevent).[1]

[1] Defendants suggest the language in the FCRA and COPPA stating the terms and provisions of the FTC Act are incorporated into those statutes requires the FTC to meet the Section 45(n) substantial injury requirement before it can enforce those statutes. *Supra* pp. 3-4. Section 45(n) places limitations on the Commission's authority to declare

These newer statutes also grant the FTC additional enforcement tools, further differentiating them from the FTC Act. Pl.'s Opp'n 10-12. As the Commission held in *LabMD*, Congress enacted the FCRA, GLBA, and COPPA to address specific concerns in particular sectors of the economy. LabMD Order 10. *See* FCRA, 15 U.S.C. § 1681a (consumer reporting agencies); GLBA, 15 U.S.C. § 6801(a) (financial institutions); COPPA, 15 U.S.C. §§ 6501-6508; 144 Cong. Rec. S12787 (daily ed. Oct. 21, 1998) (statement of Sen. Bryan, drafter and co-sponsor of COPPA) ("The goals of this legislation are: . . . to maintain the security of personally identifiable information of children collected online; and [] to protect children's privacy."). *See also* Mot. to Dismiss Hr'g Tr. 44:17-25; 45:1-22. As the Commission noted, these statutes not only impose specific regulatory requirements on companies in particular areas, but they provide the FTC with additional tools to protect consumers. *See* LabMD Order 10. One of those tools is Administrative Procedure Act rulemaking authority. *See* GLBA, 15 U.S.C. §§ 6801(b), 6805(b)(2); COPPA, 15 U.S.C. § 6502(b)(1)(D); FCRA, 15 U.S.C. § 1681w. Another tool is civil penalty authority, which is not available under Section 5. *See* FCRA, 15 U.S.C. § 1681s; COPPA, 15 U.S.C. § 6505(d). *See also* LabMD Order 10.

Moreover, as opposed to the FTC Act which merely authorizes, the FCRA, GLBA, and COPPA affirmatively compel the FTC to use its authority in particular ways. For example, COPPA instructs the FTC to promulgate rules addressing the specific duties of child-directed website operators to provide notices and obtain parental consent before collecting or disclosing children's personal information. 15 U.S.C. § 6502(b). *See also* FCRA, 15 U.S.C. § 1681w (requiring the FTC to issue regulations requiring proper disposal of consumer information); LabMD Order 10. "Of course, by *compelling* the Commission to take particular steps in those contexts, Congress did not somehow divest the Commission of its preexisting and much broader *authority* to protect consumers against 'unfair' practices." LabMD Order 13. *See also Cablevision Sys. Corp. v. FCC*, 649 F.3d 695, 705-06 (D.C. Cir. 2011).

Again, any question about the FTC's authority in the data security area is put to rest by the *LabMD* decision. In *LabMD*, the unanimous Commission specifically addressed the FCRA, GLBA, and COPPA, holding that "these laws *recognized* the Commission's *existing* enforcement authority, *expanded* that authority in particular respects, and affirmatively *directed* the Commission to take particular actions to protect consumer interests in specified contexts." LabMD Order 10. "To conclude otherwise," the Commission held, "would disregard Congress's instruction to the Commission to protect consumers from harmful practices in evolving technological and marketplace environments." *Id.* As the Commission noted, Section 5 of the FTC Act is an intentionally broad grant of power to the FTC to protect consumers from "unfair or deceptive acts or practices in or affecting commerce." *Id.* at 3-6. This grant of authority applies to *all* acts or practices in or affecting commerce. It is not limited to specific acts or practices, nor was it intended to be. *See* Pl.'s Opp'n 11. There is nothing unique about data security that exempts it from this broad authority. In fact, the Commission held, Congress intended the FTC to "ascertain, on a case-by-case basis, which specific practices should be condemned as 'unfair.'" LabMD Order 5. These findings all warrant substantial deference.

---

particular actions unfair under Section 5, either in litigation or rulemaking. It has no application where Congress itself has statutorily defined categories of actions to be unlawful and authorized the FTC to enforce those statues.

"Statutory ambiguities will be resolved, within the bounds of reasonable interpretation, not by the court but by the administering agency." *City of Arlington*, 133 S. Ct. at 1868, 1871.

B. Fair Notice

Although the Court did not request briefing on the topic, Defendants return to the untenable claim that the FTC has not satisfied due process fair notice requirements because it has not issued a comprehensive rule on data security. *Supra* pp. 4-5. This argument has no basis in the law. *See* Pl.'s Opp'n 17-25. Were Defendants correct, the FTC could never protect consumers from unfair practices without first issuing a regulation governing the specific practice at issue. Such a requirement would undermine 100 years of FTC precedent, and it would crash headlong into the Supreme Court's recognition that "the proscriptions in [Section] 5 are flexible, to be defined with particularity by the myriad of cases from the field of business," a fact that inherently requires the FTC to apply Section 5 "to the facts of particular cases arising out of unprecedented situations." *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 384-85 (1965). *See also FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 240 (1972) (Congress delegated broad authority "to the Commission to determine what practices were unfair," rather than "enumerating the particular practices to which [the term 'unfair'] was intended to apply."). Indeed, such a requirement would be an exercise in futility because "[t]here is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." *Sperry & Hutchinson Co.*, 405 U.S. at 241.

Section 45(n)'s three part test addressing when an act or practice is "unfair" adequately provides "a person of ordinary intelligence fair notice of what is prohibited" and constrains the FTC's authority to bring unfairness actions sufficiently so that the FTC may not enforce the FTC Act in a "seriously discriminatory" way. *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012). *See also* LabMD Order 15-17. Agencies routinely bring enforcement actions where the governing statute or rules lack particularized prohibitions, and instead require compliance with a general reasonableness standard like that set forth in Section 45(n). *See* Pl.'s Opp'n 23-24 (discussing the National Labor Relations Board's "good faith" requirement, and the Occupational Safety and Health Act's "general duty clause."). In fact, this Circuit has rejected fair notice challenges to similar reasonableness standards. *See Voegele Co., Inc. v. Occupational Safety & Health Review Comm'n*, 625 F.2d 1075, 1078 (3d Cir. 1980).[2]

[2] Without acknowledging the discussion of the case at the Motion to Dismiss Hearing, Defendants cite to *Secretary of Labor v. Beverly Healthcare-Hillview* ("*Beverly*"), 541 F.3d 193 (3d Cir. 2008), in baldly asserting that to satisfy fair notice requirements the FTC must provide "ascertainable certainty" of how it will enforce Section 5 unfairness. *See supra* p. 4. As the FTC explained at the hearing, however, the ascertainable certainty test set forth in *Beverly* does not apply here. *Beverly*, 541 F.3d at 202. The FTC has not given "conflicting public interpretations" of how it will apply "unfairness." Rather, the FTC has repeatedly, and publicly, explained that it will enforce unfairness consistent with the unambiguous plain terms of the statute, which defines unfair acts or practices through the Section 45(n) balancing test. *See United States v. Lachman*, 387 F.3d 42, 57 (1st Cir. 2004); Mot. to Dismiss Hr'g Tr. 72-74; Pl.'s Opp'n 13-14, 17-20. In fact, the FTC's many public complaints and consent agreements, as well as public statements and business guidance, have provided further contour to the Section 45(n) test as it is applied in the data security context. Pl.'s Opp'n 18-20. Any doubt as to whether the FTC meets fair notice here is settled in this Circuit by *Voegele*, which noted that similar "reasonable person" standards survive fair notice challenges even though they provide no guidance other than to act as a reasonable person would. 625 F.2d at 1078 (citing *B&B Insulation, Inc. v. Occupational Safety & Health Review Comm'n*, 583 F.2d 1364 (5th Cir. 1978)). *See also* LabMD Order 18-19.

Moreover, the FTC's decision to enforce the FTC Act's prohibition of unfair practices through individual enforcement actions rather than rulemaking is well within the FTC's "informed discretion." *PBW Stock Exch., Inc. v. SEC*, 485 F.2d 718, 732 (3d Cir. 1973). *See also SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947); Pl.'s Opp'n 20-22; LabMD Order 14-15. "[A]gency discretion is at its peak in deciding such matters as whether to address an issue by rulemaking or adjudication[,] [and] [t]he Commission seems on especially solid ground in choosing an individualized process where important factors may vary radically from case to case." *Am. Gas Ass'n v. FERC*, 912 F.2d 1496, 1519 (D.C. Cir. 1990).[3]

Accordingly, courts routinely uphold FTC unfairness actions despite the fact that there are no preexisting rules specifically governing the specific conduct at issue. In *FTC v. Neovi, Inc.*, 604 F.3d 1150 (9th Cir. 2010), the Ninth Circuit affirmed the district court's holding that the defendants' acts or practices related to online check drafting and delivery were unfair even though there is no specific regulation addressing the practice. The Tenth Circuit reached the same conclusion in *FTC v. Accusearch, Inc.*, 570 F.3d 1187 (10th Cir. 2009), even though no regulation explicitly prohibited the conduct in question. *See also* Pl.'s Opp'n 11. In short, Defendants' claim that the FTC must issue regulations governing data security before it may enforce its unfairness authority is inconsistent with the FTC's long enforcement history.

Moreover, as the Commission held in *LabMD*, the claim that agencies can only satisfy due process through issuing specific regulations is "particularly untenable when viewed against the backdrop of the common law of negligence. Every day, courts and juries subject companies to tort liability for violating uncodified standards of care," and when they "find that corporate defendants have violated an unwritten rule of conduct, they – unlike the FTC – can normally impose compensatory and even punitive damages." LabMD Order at 17. "There is simply no basis to conclude that the FTC's application of the Section [45](n) cost-benefit analysis violates due process, particularly where, as here, the complaint does not even seek to impose damages, let alone retrospective penalties." *Id.*[4]

For the reasons set forth above, and in prior briefing and argument, the Court should deny Defendants' Motions to Dismiss.

---

[3] Nor is that doctrine altered by the National Institute of Standards and Technology's ("NIST") critical infrastructure cyber security framework or the Department of Homeland Security's ("DHS") internal network assessment. *See supra* p. 5. The NIST framework is not an enforceable regulation requiring specific security measures. *See* Pl.'s Opp'n 16. Rather, it sets forth a voluntary *process* by which critical infrastructures can assess the threats they face and the protections they should reasonably take in response. *See, e.g.*, Exec. Order 13636, 78 FR 11737 (2013). The DHS Report is DHS's own internal assessment of its network security, and has no bearing on this case.

[4] In support of their claim that the FTC must make rules in the data security area, Defendants offer a single comment of a Congressman at a Subcommittee hearing (which in context appears actually to be about the FTC's competition-side efforts and not consumer protection unfairness actions), and an amicus brief from the U.S. Chamber of Commerce. *See supra* p. 5. Whatever weight should be accorded a single comment in a Subcommittee hearing, and an amicus brief, these statements cannot overcome the well-settled precedent holding that the FTC comports with due process even when proceeding through adjudication, rather than rulemaking. Pl.'s Opp'n 20-22.

Dated: January 21, 2014

/s/Jonathan E. Zimmerman
Lisa Weintraub Schifferle
Kristin Krause Cohen
Kevin H. Moriarty
John A. Krebs
Jonathan E. Zimmerman
Andrea V. Arias
Federal Trade Commission
600 Pennsylvania Ave., NW
Mail Stop NJ-8100
Washington, D.C. 20580

Attorneys for Plaintiff
Federal Trade Commission

/s/ Jennifer A. Hradil
Jennifer A. Hradil, Esq.
Justin T. Quinn, Esq.
GIBBONS P.C.
One Gateway Center
Newark, NJ 07102-5310
(973) 596-4500

Eugene F. Assaf, P.C., DC Bar 449778
Pro Hac Vice
K. Winn Allen, DC Bar 1000590
Pro Hac Vice
KIRKLAND & ELLIS, LLP
655 Fifteenth St. N.W.
Washington, D.C. 20005
(202) 879-5078
eugene.assaf@kirkland.com
winn.allen@kirkland.com

Douglas H. Meal, MA Bar 340971
Pro Hac Vice
David T. Cohen, MA Bar 670153
Pro Hac Vice
ROPES & GRAY, LLP
Prudential Tower, 800 Boylston Street
Boston, MA 02199-3600
(617) 951-7517
douglas.meal@ropesgray.com
david.cohen@ropesgray.com

Attorneys for Defendants

cc: Counsel via ECF

EXHIBIT 4

1023099

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

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

COMPLAINT

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

RESPONDENT'S BUSINESS

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

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

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

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

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

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

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

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

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

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

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

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

RESPONDENT'S SECURITY PRACTICES

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

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

(b) did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks. By not using measures such as penetration tests, for example, respondent could not adequately assess the extent of the risks and vulnerabilities of its networks;

(c) did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;

(d) did not adequately train employees to safeguard personal information;

(e) did not require employees, or other users with remote access to the networks, to use common authentication-related security measures, such as periodically changing passwords, prohibiting the use of the same password across applications and programs, or using two-factor authentication;

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

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

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

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

PEER-TO-PEER FILE SHARING APPLICATIONS

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

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

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

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

SECURITY INCIDENTS

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

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

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

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

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

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

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

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

VIOLATION OF THE FTC ACT

22. As set forth in Paragraphs 6 through 21, respondent's failure to employ reasonable and appropriate measures to prevent unauthorized access to personal information, including dates of birth, SSNs, medical test codes, and health information, caused, or is likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

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

NOTICE

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

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

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

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

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

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

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

ORDER

DEFINITIONS

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

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

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

3. "Affected Individual" shall mean any consumer whose personal information LabMD has reason to believe was, or could have been, accessible to unauthorized persons before the date of service of this order, including, but not limited to, consumers listed in the Insurance File and the Sacramento Documents.

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

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

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

I.

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

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

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

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

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

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

II.

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

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

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

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

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

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No.1023099. Provided, however, that in lieu of overnight courier, assessments may be sent by first-class mail, but only if an electronic version of any such assessment is contemporaneously sent to the Commission at Debrief@ftc.gov.

III.

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

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

1. a brief description of why the notice is being sent, including the approximate time period of the unauthorized disclosure, the types of personal information that were or may have been disclosed without authorization (*e.g.*, insurance information, Social Security numbers, etc.),

and the steps respondent has taken to investigate the unauthorized disclosure and protect against future unauthorized disclosures;

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

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

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

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

IV.

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

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

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

V.

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

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No. 1023099. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VII.

IT IS FURTHER ORDERED that respondent, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, they shall submit additional true and accurate written reports. Unless otherwise directed by a representative of the Commission in writing, all notices required by this Part shall be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of LabMD, Inc.*, FTC File No. 1023099.

VIII.

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

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

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

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

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

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

By the Commission.

Donald S. Clark
Secretary

EXHIBIT 5

Dissenting Statement of Commissioner J. Thomas Rosch
Petitions of LabMD, Inc. and Michael J. Daugherty
to Limit or Quash the Civil Investigative Demands

FTC File No. 1023099
June 21, 2012

I dissent from the Commission's vote affirming Commissioner Brill's letter decision, dated April 20, 2012, that denied the petitions of LabMD, Inc. and Michael J. Daugherty to limit or quash the civil investigative demands.

I generally agree with Commissioner Brill's decision to enforce the document requests and interrogatories, and to allow investigational hearings to proceed. As she has concluded, further discovery may establish that there is indeed reason to believe there is Section 5 liability regarding petitioners' security failings *independent* of the "1,718 File" (the 1,718 page 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 my view, however, as a matter of prosecutorial discretion under the unique circumstances posed by this investigation, the CIDs should be limited. Accordingly, without reaching the merits of petitioners' legal claims, I do not agree that staff should further inquire – either by document request, interrogatory, or investigational hearing – about the 1,718 File.

Specifically, I am concerned that Tiversa is more than an ordinary witness, informant, or "whistle-blower." 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. Indeed, in the instant matter, an argument has been raised that Tiversa used its robust, patented peer-to-peer monitoring technology to retrieve the 1,718 File, and then repeatedly solicited LabMD, offering

investigative and remediation services regarding the breach, long before Commission staff contacted LabMD. 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.

EXHIBIT 6

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, DC

Office of the Secretary

April 20, 2012

VIA E-MAIL AND COURIER DELIVERY

Claudia Callaway, Esq.
Christina Grigorian, Esq.
Julian Dayal, Esq.
Katten Muchin Rosenman LLP
2900 K Street, N.W.
North Tower - Suite 200
Washington, D.C. 20007
E-mail: claudia.callaway@kattenlaw.com

RE: *LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand*; and *Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand*

Dear Ms. Callaway, Ms. Grigorian, and Mr. Dayal:

On January 10, 2012, the Federal Trade Commission ("FTC" or "Commission") received the above Petitions filed by LabMD, Inc. ("LabMD") and its President, Michael J. Daugherty (collectively, "Petitioners"). This letter advises you of the Commission's disposition of the Petitions, effected through this ruling by Commissioner Julie Brill, acting as the Commission's delegate.[1]

For the reasons explained below, the Petitions are denied. You may request review of this ruling by the full Commission.[2] Any such request must be filed with the Secretary of the Commission within three days after service of this letter ruling.[3] The timely filing

[1] *See* 16 C.F.R. § 2.7(d)(4).

[2] 16 C.F.R. § 2.7(f).

[3] *Id.* This ruling is being delivered by e-mail and courier delivery. The e-mail copy is provided as a courtesy, and the deadline by which an appeal to the full Commission

of a request for review by the full Commission shall not stay the return dates established by this ruling.[4]

I. INTRODUCTION

The FTC commenced its investigation into the adequacy of LabMD's information security practices in January 2010, after a LabMD file had been discovered on a peer-to-peer ("P2P") file sharing network.[5] The file, which Petitioners call the "1,718 File" because it is 1,718 pages long, is a spreadsheet of health insurance billing information for uropathology and microbiology medical tests of around 9,000 patients. It contains highly sensitive information about these consumers, including:

- Name;
- Social Security Number;
- Date of birth;
- Health insurance provider and policy number; and
- Standardized medical treatment codes.[6]

Such information can be misused to harm consumers.

The purpose of the investigation is to determine whether Petitioners violated the FTC Act by engaging in deceptive or unfair acts or practices relating to privacy or information security. The inquiry is authorized by Resolution File No. P954807, which provides for the use of compulsory process in investigations of potential Section 5 violations involving "consumer privacy and/or data security."

---

would have to be filed should be calculated from the date on which you receive the original letter by courier delivery.

[4] *Id.*

[5] P2P programs allow users to form networks with others using the same or a compatible P2P program. Such programs allow users to locate and retrieve files of interest to them that are stored on computers of other users on the networks.

[6] LabMD Pet., Ex. C, at Fig. 4. Because the LabMD and Daugherty Petitions make the same arguments (the Petitions differ only in details about the submitter), we generally cite only to LabMD's Petition.

The investigation began with voluntary information requests for documents and information about LabMD's information security policies, procedures, practices, and training generally, as well as information about security incidents, including, but not limited to, the discovery of the 1,718 File on P2P networks. In response, LabMD produced hundreds of pages of documents, including supplements and responses to follow-up questions. To complete the investigation, staff requested issuance of CIDs to LabMD and Michael J. Daugherty, LabMD's President.

The Commission issued the CIDs on December 21, 2011. Both require testimony relating to information security policies, practices, training, and procedures. They also include a limited number of interrogatories that require Petitioners to identify documents used by the witnesses to prepare for their testimony.[7] The LabMD CID also includes a single document request asking for only those documents that were both identified in response to the CID's interrogatories and had not been previously produced to staff.[8]

Petitioners seek to quash or limit the CIDs because, they claim, the CIDs "appear to be premised on" the download of the 1,718 File (hereinafter, the "File disclosure").[9] Their principal objection relates to the merits of the investigation. In particular, they contend (without citing any authority) that the Commission must have a "justifiable" belief that a law violation has occurred before it can issue CIDs, and that the File disclosure cannot support such a belief. They claim that the File disclosure occurred not because LabMD failed to implement reasonable and appropriate security measures, but because the company was the victim of an illegal intrusion conducted by Tiversa (a P2P information technology and investigation services company) and Dartmouth College faculty using Tiversa's powerful P2P searching technology.[10] Further, Petitioners argue that no actual harm to consumers resulted from the File disclosure.[11] Accordingly, they

[7] LabMD Pet., Ex. A.

[8] LabMD Pet., Ex. A.

[9] LabMD Pet., at 1.

[10] Petitioners claim that in the course of a Department of Homeland Security-funded research project, Professor M. Eric Johnson of Dartmouth College's Tuck School of Business and Tiversa used Tiversa's P2P searching technology to search for and then download the file. LabMD Pet., at 3-4, 7, & Ex. F, at 10-12.

[11] The Petitions claim that there is no allegation of actual consumer injury from the File disclosure. LabMD Pet., at 7.

contend that investigating either the File disclosure or the adequacy of LabMD's security practices is improper because no law violation can have occurred, and that the CIDs therefore should be quashed.[12]

As discussed below, these arguments are undermined by: (1) the obvious point that an investigation necessarily must precede assessment of whether there is reason to believe a law violation may have occurred (in any matter); (2) the scope of the authorizing resolution; and (3) the language of the FTC Act. The resolution authorizes use of compulsory process in an investigation to determine whether Petitioners engaged in deceptive or unfair practices related to privacy or security. Petitioners' focus on the File disclosure is misplaced – it may bear on the adequacy of LabMD's security practices under the FTC Act but does not establish the investigation's scope under the resolution.[13] Further, in such an investigation Section 5 directs the Commission to consider whether security practices are unfair because they create a sufficient risk of harm, even if no harm has been reported.

Petitioners make two additional arguments in support of their Petitions. First, they argue that the resolution authorizing the CIDs did not provide them with sufficient notice of the purpose and scope of the investigation. Second, they argue that the FTC is without jurisdiction to pursue this investigation. Both of these additional arguments are equally without merit.

II. ANALYSIS

A. The applicable legal standards.

Compulsory process such as a CID is proper if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant to the inquiry, as that inquiry is defined by the investigatory resolution.[14]

---

[12] LabMD Pet., at 7-8.

[13] *See, e.g.*, *CVS Caremark Corp.*, No. 072-3119, at 4 (Dec. 3, 2008) (confirming that the scope of an investigation authorized by Resolution P954807 properly included all of CVS' "consumer privacy and data security practices" (including its computer security practices) and could not be limited (as the company argued) to just known incidents of unauthorized disposal of paper documents in dumpsters).

[14] *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950); *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1088 (D.C. Cir. 1992); *FTC v. Texaco, Inc.*, 555 F.2d 862, 874 (D.C. Cir. 1977).

Agencies have wide latitude to determine what information is relevant to their law enforcement investigations and are not required to have "a justifiable belief that wrongdoing has actually occurred," as Petitioners claim.[15] As the D.C. Circuit has stated, "The standard for judging relevancy in an investigatory proceeding is more relaxed than in an adjudicatory one . . . . The requested material, therefore, need only be relevant to the *investigation* – the boundary of which may be defined quite generally, as it was in the Commission's resolution here."[16] Agencies thus have "extreme breadth" in conducting their investigations,[17] and "in light of [this] broad deference . . ., it is essentially the respondent's burden to show that the information is irrelevant."[18]

B. The CIDs satisfy the foregoing standards.

Petitioners argue that the CIDs are improper for several reasons. In particular, they claim no law violation could have occurred, by arguing that: (1) not even "perfect" security measures (let alone the reasonable security measure standard the Commission uses to determine whether a law violation may have occurred) could have prevented the File disclosure because Tiversa's technology "can penetrate even the most robust network security,"[19] and (2) no actual injury resulted from the File disclosure.

---

[15] LabMD Pet., at 6. *See, e.g.*, *Morton Salt*, 338 U.S. at 642-43 ("[Administrative agencies have] a power of inquisition, if one chooses to call it that, which is not derived from the judicial function. It is more analogous to the Grand Jury, which does not depend on a case or controversy for power to get evidence but can investigate merely on suspicion that the law is being violated, or even just because it wants an assurance that it is not.").

[16] *Invention Submission*, 965 F.2d at 1090 (emphasis in original, internal citations omitted) (citing *FTC v. Carter*, 636 F.2d 781, 787-88 (D.C. Cir. 1980), and *Texaco*, 555 F.2d at 874 & n.26).

[17] *Linde Thomsen Langworthy Kohn & Van Dyke, P.C. v. Resolution Trust Corp.*, 5 F.3d 1508, 1517 (D.C. Cir. 1993) (citing *Texaco*, 555 F.2d at 882).

[18] *Invention Submission*, 965 F.2d at 1090 (citing *Texaco*, 555 F.2d at 882) ("burden of showing that the request is unreasonable is on the subpoenaed party"). *Accord FTC v. Church & Dwight Co.*, 756 F. Supp. 2d 81, 85 (D.D.C. 2010).

[19] LabMD Pet., at 7.

The Commission is not required, as a precondition to conducting a law enforcement investigation, to make a showing that it is likely that a law violation has occurred. The D.C. Circuit confirmed this point in *FTC v. Texaco, Inc.*, when it stated, "[I]n the pre-complaint stage, an investigating agency is under no obligation to propound a narrowly focused theory of a possible future case . . . . The court must not lose sight of the fact that the agency is merely exercising its legitimate right to determine the facts, and that a complaint may not, and need not, ever issue."[20] Here, Petitioners seek to quash the CIDs by asserting that LabMD's practices must have been reasonable under the FTC Act because the 1,718 File was retrieved using Tiversa's powerful searching technology. Accepting this argument would prevent the Commission from exploring relevant issues bearing on reasonableness, such as, for example, whether the company's security practices could have prevented the 1,718 File from being retrieved using the common P2P programs that are used by millions of computer users each day or whether there were readily available security measures LabMD did not implement that would have prevented even Tiversa's technology from successfully retrieving the file. Although such evidence (if it exists at all) could undermine their reasonableness claim, Petitioners nonetheless argue that the Commission cannot use CIDs to investigate whether the evidence exists unless it already has reason to believe it does exist. For this reason, Petitioners' argument that the strength of Tiversa's P2P searching technology precludes the possibility that a law violation occurred, regardless of the state of LabMD's security, must fail.

Similarly, Petitioners' assertion that no law violation can have occurred because no actual harm has been shown also fails because, under Section 5, 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.[21]

Both arguments conflate the purpose of a CID with the purpose of a future potential complaint. A CID can only compel information necessary for an investigation, and the investigation may or may not result in allegations of a law violation.[22]

---

[20] 555 F.2d 862, 874 (D.C. Cir. 1977). This holding from *Texaco* has been repeatedly reaffirmed, most recently in *FTC v. Church & Dwight*, 747 F. Supp. 2d 3, 6, *aff'd*, 2011 U.S. App. LEXIS 24587 (D.C. Cir. Dec. 13, 2011).

[21] 15 U.S.C. § 45(n) (an unfair practice is one that "causes or *is likely to cause* substantial injury to consumers"); *see also* FTC Policy Statement on Unfairness, 104 F.T.C. 949, 1073 & n.15 (1984).

[22] Petitioners also argue that the CIDs are improper for other reasons. They claim that because security issues posed by P2P programs were common (according to Tiversa), such issues could not constitute an unfair or deceptive practice in violation of the FTC

Additionally, Petitioners have claimed that the CIDs are burdensome, but they have not come forward with any support for these assertions. Instead, they make only bald statements that the CIDs are "highly burdensome," "unduly burdensome," "costly and burdensome," and "deeply burdensome."[23] Having offered no factual information about the alleged burdens of complying with the CIDs, Petitioners have not sustained their burden to demonstrate that the CIDs are unduly burdensome.[24]

Such a showing would be difficult here in any event. Notwithstanding Petitioners' description, the CIDs call primarily for testimony, not documents. Thus, it seems unlikely that compliance would require large-scale or time-consuming document production.

Act. LabMD Pet., at 7-8 & n.34. This argument is unavailing. The fact that a particular practice may be pervasive or widespread has no bearing on whether the FTC may investigate it as also deceptive or unfair. Indeed, accepting Petitioners' argument would confine the FTC to investigating only those activities that were rare or uncommon, thus crippling the agency's law enforcement mission. Along the same lines, Petitioners contend that the risks of P2P technology, and the resulting potential liabilities to businesses, were not known in 2008, when the File disclosure occurred. In support of this claim, they assert that the FTC did not notify businesses or publish guidance about P2P until 2010. LabMD Pet., at 8. In fact, many, including the FTC, warned about the risks presented by P2P programs years before the File disclosure occurred. *See, e.g.*, FTC Staff Report, "Peer-to-Peer File Sharing Technology: Consumer Protection and Competition Issues" (June 2005), available at http://www.ftc.gov/reports/ p2p05/050623p2prpt.pdf; Prepared Statement of the Federal Trade Commission Before The Committee on Oversight and Government Reform, United States House of Representatives (July 24, 2007) (discussing P2P programs and risks), available at http://www.ftc.gov/os/testimony/P034517p2pshare.pdf.

[23] LabMD Pet., at 7, 9, & 10.

[24] *See, e.g.*, *Texaco*, 555 F.2d at 882 ("The burden of showing that the request is unreasonable is on the subpoenaed party.") (citing *United States v. Powell*, 379 U.S. 48, 58 (1964)); *accord EEOC v. Maryland Cup Corp.*, 785 F.2d 471, 476 (4th Cir. 1986) (subpoena is enforceable absent a showing by recipient that the requests are unduly burdensome); *FTC v. Standard American, Inc.*, 306 F.2d 231, 235 (3d Cir. 1962) (recipient has responsibility to show burden and must make "a record . . . of the measure of their grievance rather than ask [the court] to assume it"); *In re Nat'l Claims Serv., Inc.*, 125 F.T.C. 1325, 1328-29 (1998) (FTC ruling that petition to quash must substantiate burden with specific factual detail).

Furthermore, to the extent that the CIDs call for narrative responses, they merely require Petitioners to identify documents related to the requested testimony. In fact, there is only one specification that requires the production of documents, and even that specification is limited to documents identified in response to the interrogatories to the extent they were "not already been produced to the FTC."[25]

Finally, Petitioners, without explaining its relevance, contend that the timing of the CIDs is "troubling," coming after LabMD's conduct had been reviewed by two congressional committees, and after LabMD filed suit against Tiversa and others alleging conversion and trespass, among other violations, based on the File disclosure in 2008.[26] Though Petitioners seem to believe that there is some connection between their rejection of Tiversa's offer to provide LabMD with information security services, their subsequent lawsuit, and the FTC's investigation, the chronology of the investigation does not support such a conclusion. The FTC first contacted LabMD for information in January 2010, well before LabMD filed its lawsuit against Tiversa in October 2011.[27] Moreover, the claim that LabMD's conduct was reviewed by congressional committees does not appear to be based on evidence presented in the Petitions. Although Petitioners have attached as exhibits three instances of congressional testimony by Tiversa, none identifies LabMD by name or discusses the specifics of the File disclosure.

C. The resolution provides sufficient notice of the purpose and scope of the FTC's investigation.

Under the FTC Act, a CID is proper when it "state[s] the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation."[28] It is well-established that the resolution authorizing the process provides the requisite statement of the purpose and scope of the investigation,[29]

---

[25] LabMD Pet., Ex. A.

[26] LabMD Pet., at 9 & Ex. F.

[27] We note further that this suit came more than three years after the solicitations Petitioners complain of in their Petitions. LabMD Pet., Ex. F, at 1, 17-23.

[28] 15 U.S.C. § 57b-1(c)(2).

[29] *Invention Submission.*, 965 F.2d at 1088; *accord Texaco*, 555 F.2d at 874; *FTC v. Carter*, 636 F.2d 781, 789 (D.C. Cir. 1980); *FTC v. Anderson*, 631 F.2d 741, 746 (D.C. Cir. 1979).

and also that the resolution may define the investigation generally, need not state the purpose with specificity, and need not tie it to any particular theory of violation.[30]

Despite this, Petitioners object that Resolution File No. P954807 did not provide sufficient notice of the purpose and scope of the investigation, and they further claim that this resolution is inadequate under the standard developed by the D.C. Circuit in *FTC v. Carter*, 636 F.2d 781, 788 (D.C. Cir. 1980).[31]

Petitioners' first argument reads the governing standard too narrowly. Resolution File No. P954807 authorizes the use of compulsory process:

> 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, 15 U.S.C. § 45, as amended.[32]

This general statement of the purpose and scope of the investigation is more than sufficient under the standard for such resolutions, and courts have enforced compulsory process issued under similarly broad resolutions.[33]

Petitioners' reliance on *Carter* is also misplaced. While *Carter* held that a bare reference to Section 5, without more, "would not serve very specific notice of purpose," the Court approved the resolution at issue in that case, noting that it also referred to specific statutory provisions of the Cigarette Labeling and Advertising Act, and further

---

[30] *Invention Submission*, 965 F.2d at 1090; *Texaco*, 555 F.2d at 874 & n.26; *FTC v. Nat'l Claims Serv., Inc.*, No. S 98-283 FCD DAD, 1999 WL 819640, at *2 (E.D. Cal. Feb. 9, 1999) (citing *EPA v. Alyeska Pipeline Serv. Co.*, 836 F.2d 443, 477 (9th Cir. 1988)).

[31] LabMD Pet., at 10-12.

[32] LabMD Pet., Ex. A.

[33] *See FTC v. Nat'l Claims Serv.*, 1999 WL 819640, at *2 (finding omnibus resolution referring to FTC Act and Fair Credit Reporting Act sufficient); *FTC v. O'Connell Assoc., Inc.*, 828 F. Supp. 165, 171 (E.D.N.Y. 1993) (enforcing CIDs issued pursuant to omnibus resolution). The Commission has repeatedly rejected similar arguments about such omnibus resolutions. *See, e.g.*, *Firefighters Charitable Found.*, No. 102-3023, at 4 (Sept. 23, 2010); *D. R. Horton, Inc.*, Nos. 102-3050, 102-3051, at 4 (July 12, 2010); *CVS Caremark Corp.*, No. 072-3119, at 4 (Dec. 3, 2008).

related it to the subject matter of the investigation.[34] With this additional information, the Court felt "comfortably apprised of the purposes of the investigation and the subpoenas issued in its pursuit . . . ."[35]

The resolution here, like the one in *Carter*, does not cite solely to Section 5, but also recites the subject matter of the investigation: "deceptive or unfair acts or practices related to consumer privacy and/or data security." Since the resolution here discloses the subject matter of the investigation in addition to invoking Section 5, the resolution provides notice sufficient under *Carter* of the purpose and scope of the investigation.

As a final note, the history of the investigation itself undermines Petitioners' argument that the present CIDs do not sufficiently advise them of the nature and scope of the investigation. Petitioners have been under investigation since January 2010 and have engaged in repeated discussions with staff. At no point have Petitioners indicated they did not understand the purpose or scope; in fact, Petitioners have already produced hundreds of pages of documents in response to staff requests. Moreover, the Petitions under consideration here present highly detailed and factual arguments going to the very merits of the investigation. The Commission has previously found that such interactions may be considered along with the resolution in evaluating the notice provided to Petitioners.[36]

D. Petitioners' challenge to the FTC's regulatory authority is premature and without basis.

Petitioners' final argument is that the FTC lacks jurisdiction to conduct the instant investigation.[37] Petitioners assert that LabMD is a health care company and that the

---

[34] *Carter*, 636 F.2d at 788.

[35] *Id.*

[36] *Assoc. First Capital Corp.*, 127 F.T.C. 910, 915 (1999) ("[T]he notice provided in the compulsory process resolutions, CIDs and other communications with Petitioner more than meets the Commission's obligation of providing notice of the conduct and the potential statutory violations under investigation.").

[37] Petitioners also claim that the resolution does not meet the requirements established by the FTC's Operating Manual. LabMD Pet., at 10. As discussed above, by disclosing the statutory basis and subject matter of the investigation, the resolution does provide notice as required by the Operating Manual. That said, the Operating Manual, by its own terms, is advisory. It is not a "basis for nullifying any action of the Commission or the staff."

information disclosed in the 1,718 File is protected health information ("PHI") under the Health Insurance Portability and Accountability Act ("HIPAA"). Accordingly, they contend, the adequacy of their security practices with respect to this information is subject to the exclusive jurisdiction of HHS.[38]

As an initial matter, it is well-established that challenges to the FTC's jurisdiction are not properly raised through challenges to investigatory process. As the D.C. Circuit stated: "Following *Endicott* [*Johnson Corp. v. Perkins*, 317 U.S. 501, 509 (1943)], courts 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."[39] The reasons for such a rule are obvious. If a party under investigation could raise substantive challenges in an enforcement proceeding, before the agency has obtained the information necessary for its case – essentially requiring the FTC to litigate an issue before it can learn about it – then the FTC's investigations would be foreclosed or substantially delayed.[40] Thus, Petitioners' basic challenge to the FTC's jurisdiction is premature and will not support quashing the instant CIDs.

In any event, the claim that HHS has exclusive jurisdiction to investigate privacy and data security issues involving PHI is without basis. Petitioners essentially invoke the doctrine of implied repeal to assert that HIPAA and its Privacy and Security Rules displace FTC jurisdiction. But implied repeal is "strongly disfavored," for two reasons.[41] First, courts have recognized that agencies may have overlapping or concurrent jurisdiction, and thus that the same issues may be addressed and the same parties

---

Operating Manual, § 1.1.1.1. *See also FTC v. Nat'l Bus. Consultants, Inc.* 1990 U.S. Dist. LEXIS 3105, 1990-1 Trade Cas. (CCH) ¶68,984, at *29 (E.D. La. March 19, 1990).

[38] LabMD Pet., at 12-13.

[39] *FTC v. Ken Roberts Co.*, 276 F.3d 583, 586 (D.C. Cir. 2001) (citing *United States v. Sturm, Ruger & Co.*, 84 F.3d 1, 5 (1st Cir. 1996)); *United States v. Construction Prods. Research, Inc.*, 73 F.3d 464, 468-73 (2d Cir. 1996); *EEOC v. Peat, Marwick, Mitchell & Co.*, 775 F.2d 928, 930 (8th Cir. 1985); *Donovan v. Shaw*, 668 F.2d 985, 989 (8th Cir. 1982); *FTC v. Ernstthal*, 607 F.2d 488, 490 (D.C. Cir. 1979); *accord Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 213-14 (1946).

[40] *Texaco*, 555 F.2d at 879.

[41] *Galliano v. United States Postal Serv.*, 836 F.2d 1362, 1369 (D.C. Cir. 1988).

proceeded against simultaneously by more than one agency.[42] Second, courts rarely hold that one federal statute impliedly repeals another because "'when two statutes are capable of co-existence, it is the duty of the courts . . . to regard each as effective.'"[43] Thus, repeals by implication will only be found where the Congressional intent to effect such a repeal is "clear and manifest."[44]

Petitioners can point to no such "clear or manifest" evidence that Congress intended HIPAA or its rules to displace the FTC Act. The authority Petitioners cite for the proposition that HHS has exclusive jurisdiction does not address such repeal.[45] To the contrary, there is ample evidence against such implied repeal. For one, the same authority cited by Petitioners – the preamble to the Privacy Rule – expressly provides that entities covered by that Rule are "also subject to other federal statutes and regulations."[46] Also, this preamble includes an "Implied Repeal Analysis," which is silent as to any implied repeal of the FTC Act.[47] Recent legislation shows that, if anything, Congress intended the FTC and HHS to work collaboratively to address potential privacy and data security risks related to health information. The American Recovery and Reinvestment Act of 2009, for instance, required HHS and the FTC to develop harmonized rules for data breach notifications by HIPAA-covered and non-HIPAA-covered entities, respectively. *See* 74

---

[42] *FTC v. Cement Inst.*, 333 U.S. 683, 694 (1948); *see also Texaco*, 555 F.2d at 881 ("[T]his is an era of overlapping agency jurisdiction under different statutory mandates."); *Thompson Med. Co. v. FTC*, 791 F.2d 189, 192 (D.C. Cir. 1986). Because agencies have overlapping jurisdiction, they often work together. For instance, the FTC and HHS collaborated on the investigation of CVS Caremark Corporation. *See CVS Caremark Corp.*, No. 072-3119, at 7 (Aug. 6, 2008).

[43] *Radzanower v. Touche Ross & Co.*, 426 U.S. 148, 155 (1976) (quoting *Morton v. Mancari*, 417 U.S. 535, 551 (1974)).

[44] *Id.* at 154.

[45] LabMD Pet., at 12 (citing 65 Fed. Reg. 82,462, 82,472 (Dec. 28, 2000)). This Federal Register notice is the Notice of Public Rulemaking for the Privacy and Security Rules under HIPAA. The excerpt cited by Petitioners does not address the scope of HHS' enforcement jurisdiction, but rather discusses the delegation of enforcement authority from the Secretary of HHS to HHS' Office for Civil Rights. 65 Fed. Reg. 82,472 (Dec. 28, 2000).

[46] 65 Fed. Reg. 82,462, 82,481 (Dec. 28, 2000).

[47] *Id.* at 82,481-487.

Fed. Reg. 42,962, 42,962-63 (Aug. 25, 2009). Thus, HIPAA and its Rules do not serve to repeal FTC jurisdiction, which is overlapping and concurrent to HHS'.

This is particularly appropriate where, as here, the consumer information at issue included more than just health information. The consumer information exposed in the 1,718 File also included names, Social Security numbers, and dates of birth. While this information can be considered PHI under HIPAA when combined with health information, the information clearly exposes consumers to the risk of identity theft and is exactly the kind of sensitive personal information that the Commission is charged with protecting under Section 5 of the FTC Act and other statutes. Petitioners have provided no proper basis to challenge the investigation as an exercise of the Commission's jurisdiction under these authorities.

III. CONCLUSION AND ORDER

For the foregoing reasons, **IT IS HEREBY ORDERED THAT** LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand be, and hereby is, **DENIED**; and

IT IS FURTHER ORDERED THAT Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand be, and hereby is, **DENIED**; and

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); 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 now be produced on or before May 11, 2012.

By direction of the Commission.

Donald S. Clark
Secretary

EXHIBIT 7

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 8

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 9

In the Matter of:

LabMD, Inc.

September 25, 2013
Initial Pretrial Conference

Condensed Transcript with Word Index

For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

I N D E X

CASE OVERVIEW: PAGE:
BY MR. SHEER 8
BY MR. RUBINSTEIN 22

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of:)
LABMD, INC.,) Docket No. 9357
a corporation.)
)

INITIAL PRETRIAL CONFERENCE
SEPTEMBER 25, 2013
2:00 P.M.
PUBLIC SESSION

BEFORE THE HONORABLE D. MICHAEL CHAPPELL
Administrative Law Judge

Reported by: Susanne Bergling, RMR-CRR-CLR

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:
ALAIN SHEER, ESQ.
LAURA RIPOSO VANDRUFF, ESQ.
MEGAN COX, ESQ.
MARGARET LASSACK, ESQ.
RYAN MEHM, ESQ.
Federal Trade Commission
Division of Privacy and Identity Protection
601 New Jersey Avenue, N.W.
Washington, D.C. 20001
(202) 326-2999
asheer@ftc.gov

ON BEHALF OF RESPONDENT:
REED D. RUBINSTEIN, ESQ.
Dinsmore & Shohl LLP
801 Pennsylvania Avenue, N.W., Suite 610
Washington, D.C. 20004
(202) 372-9100
reed.rubinstein@dinsmore.com

ALSO PRESENT:
Victoria Arthaud and Hillary Sloane Gebler

P R O C E E D I N G S
- - - - -

JUDGE CHAPPELL: Okay. Call to order Docket 9357, In Re: LabMD. Is there a space after the B or is that one word, "LabMD"?

MR. RUBINSTEIN: It is one word, Your Honor.

JUDGE CHAPPELL: Okay. Thank you.

I will start with appearances of the parties, and I will start with the Government. Go ahead.

MR. SHEER: Good afternoon, Your Honor. I'm Alain Sheer representing the Commission.

MS. VANDRUFF: Good afternoon, Your Honor. Laura VanDruff, Complaint Counsel.

JUDGE CHAPPELL: Okay.

And for Respondent?

MR. RUBINSTEIN: Your Honor, Reed Rubinstein representing Respondent. If I could, I would like to take this opportunity to thank you and to thank government counsel for their accommodation of my schedule. It is very much appreciated.

JUDGE CHAPPELL: You're welcome. I would expect that request to come a little sooner next time.

MR. RUBINSTEIN: Yes, Your Honor.

JUDGE CHAPPELL: And also, just so everyone knows, we do follow motions practice, and I will need a

motion from here out to deal with something.
MR. RUBINSTEIN: Thank you.
JUDGE CHAPPELL: I notice that we have got more than two people listed at on least one side. Our office will email courtesy copies of orders to the parties. That's courtesy copies. Official service is made by the Office of the Secretary. I will need each party to designate no more than two individuals to receive communications from my office. You can send an email to my assistant, Dana Gross, or just to the OALJ Web site, and give us the two people you want to receive courtesy copies from my office.
I think for the first time in history we have no modifications to the draft scheduling order. So, thanks to both of you. I will issue that order by tomorrow or Friday. I think I'm obligated to get it out by Friday under the latest rules.
There's a limit to the amount of time we're in trial. I don't anticipate us getting anywhere near the limit. Does -- while we're here, how many witnesses do you anticipate for the Government? I just need a ballpark. I'm not holding you to anything.
MR. SHEER: Judge, I'm watching the monitor. We expect that we will be putting on seven or eight witnesses.

JUDGE CHAPPELL: Okay.
And for the Respondent?
MR. RUBINSTEIN: Approximately the same number.
JUDGE CHAPPELL: I'm thinking this is going to move along fairly quickly. Any experts?
MR. SHEER: Yes, Your Honor. We are going to be using experts on technical issues and also on consumer injury.
JUDGE CHAPPELL: You need to stand up when you speak. She needs to hear you. Use that microphone.
MR. SHEER: Sorry. We are expecting to use technical experts and also experts for consumer injury.
JUDGE CHAPPELL: Okay.
MR. RUBINSTEIN: Your Honor, we also will be using --
JUDGE CHAPPELL: If you -- if you use that microphone -- just stand and use one of the microphones, either one. You have got one over in the middle.
MR. RUBINSTEIN: This one works, if it works for you.
We will also be presenting expert testimony, rebuttal testimony to the Government's witnesses. We anticipate there will be two, perhaps three, that will go to harm and will also go to the technical issues associated with the file theft.

JUDGE CHAPPELL: Okay. Under the current rules, the hearing is limited to no more than 210 hours. So, I need the parties to develop a system or mechanism to keep track of that, although I don't see us stretching those boundaries in this hearing.
Regarding -- one thing regarding the scheduling order, let me talk about dispositive motions. I didn't put a deadline on the scheduling order for summary judgment motions. There is a rule that covers that, if you intend to file a summary judgment, and if you don't know, I'll tell you.
Summary judgments will be ruled on by the Commission, the same body that voted to issue the complaint in this case. With respect to motion to dismiss or other substantive motion, the rules provide that if they are filed before the start of the evidentiary hearing, they will be ruled on by that same Commission; however, motions to dismiss or substantive motions filed after the start of the evidentiary hearing will be decided by me, not the Commission.
Have there been any settlement discussions?
MR. SHEER: There were very, very preliminary settlement discussions; that is to say that Respondent LabMD had indicated they had interest in settlement at one point long ago, but the parties did not pursue it,

and at this moment, there are no settlement discussions on the table or ongoing.
JUDGE CHAPPELL: Any comment on that?
MR. RUBINSTEIN: That is correct, Your Honor.
JUDGE CHAPPELL: At this time, I allow each side to present an overview of their case, and I limit it to 15 minutes, and I'll let the Government go first; however, I'll let you know, if I ask questions, I will add to your time, or take up any of your 15 minutes.
Go ahead.
MR. SHEER: Thank you, Your Honor. LabMD is a medical laboratory that tests blood and tissue samples that doctors take from consumers. In doing so, it's collected very sensitive information about hundreds of thousands of consumers, including names, Social Security numbers, checking account information, and medical test results.
JUDGE CHAPPELL: Hundreds of thousands. So, you're saying they do a national business?
MR. SHEER: They do a national business.
LabMD exposes this treasure trove of information to people who never should have had access to it by failing to take reasonable and appropriate security measures. Identity thieves use consumers' personal information to impersonate them in a variety of ways,

9

depending on the information. For example, financial information has been misused to open new -- to conduct credit card fraud and to go into bank accounts; and medical information has been misused to steal insurance benefits. In each of the last ten years, identity theft has been the number one complaint that the FTC has received. There were 369,000 complaints in 2012.

The personal information that LabMD maintains is information that identity thieves want. This was action was brought under Section 5 of the FTC Act. Section 5 provides the Commission with broad authority to address new areas and practices as they develop.

JUDGE CHAPPELL: Have you -- in that regard, has the Commission issued guidelines for companies to utilize to protect this information or is there something out there for a company to look to?

MR. SHEER: There is nothing out there for a company to look to. 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.

In addition, there have been public statements made by the Commission, as well as educational materials that have been provided. And in addition, the industry,

10

the IT industry itself, 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, with one exception, and the exception is that the Commission's process as to the calculation of the potential consumer harm from unauthorized disclosure of information.

JUDGE CHAPPELL: Is there a rulemaking going on at this time or are there rules that have been issued in this area?

MR. SHEER: There are no -- there is no rulemaking, and no rules have been issued, other than the rule issued with regard to the Gramm-Leach-Bliley Act. There is a safeguards rule there which is issued for financial institutions. The way that rule reads and the way it works, it basically --

JUDGE CHAPPELL: The FTC has jurisdiction in that area?

MR. SHEER: It has jurisdiction over certain types of financial institutions, such as --

JUDGE CHAPPELL: Is that expressed in that Act?

MR. SHEER: It is.

JUDGE CHAPPELL: Okay.

MR. SHEER: As I was saying, Your Honor, information security, which is an essential part of our

11

economy now given the increasing reliance on and use of computer networks, is one of the new areas that the Commission is able to look into. The complaint alleges that the company, LabMD, engaged in an unfair act or practice in violation of Section 5 by collecting and storing large amounts of very sensitive consumer information and failing to use reasonable and appropriate security measures to prevent the information from being disclosed without authorization.

As set out in 15 USC 45(n), an act or practice is unfair when it causes or is likely to cause substantial consumer injury that is not -- and the injury is not reasonably avoidable by consumers and not offset by countervailing benefits to consumers or competition. The complaint alleges that LabMD systematically failed to practice what IT professionals generally call -- quote unquote -- defense in depth.

Defense in depth is a general approach for identifying the kinds of security measures that will be reasonable under particular circumstances. It sets out guiding principles that IT professionals and industry have known and used for years. There are lots of sources for the principles, such as materials published by the National Institute of Standards and Technology, continuing education for IT professionals, practical IT

12

experience, and lessons learned from publicized breaches.

Some of these guiding principles are, first, do not put all your eggs in one basket, because a single security measure may fail or be vulnerable. For example, if the only security measure for a company's network were a firewall and the firewall were not set up correctly, an outsider could exploit the mistake and gain entry to the network, because there are no other security measures in place. The outsider would have free reign within the network and could find -- easily find and export sensitive information.

Second, limit a computer user's control over the computers and data to the lowest level the user needs to perform their job. For example, users do not need to be able to change security settings on their computers or install programs on their computers without getting prior approval.

Third, also use nontechnical measures, such as providing security training for employees, a plan for responding to security incidents, and maintaining written security policies and procedures for IT employees to follow.

The final step in identifying measures that will provide reasonable defense in depth is a common sense

13

balancing of the costs and benefits of available security measures. The balancing process is very similar to how businesses decide sometimes whether to purchase new equipment, except that it includes the potential loss from disclosing the company's business plans, for example. This is called risk management, management by IT professionals and industry.

The Commission's cases set out this same approach for analyzing the reasonableness of security measures with one possible difference. The possible difference is that the Commission's approach takes into account potential consumer harm from unauthorized disclosure of the information.

So, you might ask, how hard is it to do this? In many instances, it will be relatively easy to qualitatively balance cost and benefit using risk management concepts. Consider the following hypothetical. A company uses a program to store thousands of consumer names and Social Security numbers. A vulnerability in the program was discovered and made public a year ago. At the time, IT professionals classified the vulnerability as a 10 risk on a scale of 1 to 10, with 10 being the most critical risk.

In less than an hour, an IT employee could fix the vulnerability by installing a free update that was

14

made available when the vulnerability was first discovered, and the company didn't do so. The potential loss is very high for this hypothetical. The vulnerability is critical, and disclosing names and Social Security numbers could cause considerable consumer harm. On the other hand, the cost to having an IT professional install the free update is very low. Because the potential consumer loss obviously far exceeds the cost of installing the update, it's unreasonable not to do so.

Applying these concepts, LabMD did not pass Defense in Depth 101, not just in one way, but in a number of ways. As set out in paragraph 10 of the complaint, the company failed to identify commonly known or reasonably foreseeable risks to personal information. It did not adequately train employees about security risks and practices. It did not appropriately limit employee access to just the information they needed to do their jobs.

It did not correctly or appropriately authenticate users to verify that they are who they say they are. It did not adequately update computer operating systems and equipment. And it did not take reasonable measures to prevent and detect unauthorized access to personal information. And finally, it did not

15

implement a comprehensive information security program.

LabMD systematically failed to use reasonable security measures to protect very sensitive information. I'd like to talk about two of them in a little more depth. The first is the company's failure to use appropriate measures to prevent and detect unauthorized access to consumer information, as happened here when a LabMD file was shared through a peer-to-peer file-sharing network without alarm bells going at off the company. The network is called peer-to-peer, or P2P, because users can share files directly from their own computers to the computers of other people on the network.

The complaint alleges in paragraph 18 that a P2P program called Limewire was installed on a LabMD computer used by the company's billing manager. Limewire allows users, like the billing manager, to select files on their computers to make available to other Limewire users. Hundreds of files on the billing manager's computer were available through Limewire, including some business files.

One business file that was available and shared contained highly sensitive information about approximately 9300 consumers, including their names, Social Security numbers, dates of birth, health

16

insurance provider names and policy numbers, and standardized medical treatment codes. This is the kind of information that can easily be misused to conduct new account fraud and medical identity theft and disclosing treatment codes that may cause privacy harms.

Limewire does present a risk that files that should not be shared will be shared inadvertently with other Limewire users, as likely happened here. The irony is that LabMD had no need to accept this risk, because it admittedly had no need for Limewire. The company could have addressed the risk very easily, but it didn't. If it had, it could have stopped Limewire from being downloaded; it could have prevented or detected its installation on the LabMD computer; and it would have been alerted when files were shared so that it could stop the sharing.

It's no excuse here that the billing manager should not have been using Limewire in the first place. People are known to make mistakes and to use programs that they shouldn't, which is why technical security measures or controls are needed to achieve defense in depth.

JUDGE CHAPPELL: Limewire, is this something that is free or was it purchased?

MR. SHEER: Our understanding is that it was

free.

I'd like to turn to the second failure, and that is the failure to use appropriate measures to identify commonly known or reasonably foreseeable risks to personal information as set out in paragraph 10 of the complaint. Because no single tool can identify all the different security threats a company may face, IT professionals tell us that identifying risks usually requires a variety of measures or tools.

One such tool that's familiar to almost all of us is an antivirus program. Another tool is called a penetration test, which usually includes an automated vulnerability scan and related activities. Pen tests, as they're called, probe a company's defenses from the outside looking for cracks, just like an intruder would.

A pen test might, again, by looking for a vulnerability in a firewall, looking to test the firewall for a vulnerability, looking for an opening, basically, to get into the network. Once inside the network, the test might test computers and applications or programs, looking for vulnerabilities that could be leveraged to get access to sensitive information.

We are told that antivirus programs can't identify holes in firewalls and that pen tests can't identify viruses. Both of them are needed to

effectively identify risks in networks that connect online like LabMD's. Both are basic, foundational tools that have been used by companies for years.

JUDGE CHAPPELL: You're talking about antivirus, but if you have a P2P program, you've created the hole. So, how is your antivirus going to stop something that you've created? What's the point of that?

MR. SHEER: That's exactly the point. The point is that the antivirus program is not going to identify the P2P application or program that's on your network.

JUDGE CHAPPELL: It's like clicking on the link on the email you shouldn't open. Your Norton Antivirus isn't going to stop that because you clicked.

MR. SHEER: You're preaching to the choir, yes.

JUDGE CHAPPELL: Well, not necessarily. I'm objective here. My point is, why would I pay for extra antivirus software if I've decided to use P2P software and I know the hole is there? What's the point in telling me I needed to put antivirus on my computer?

MR. SHEER: Well, we're not making the argument that they should have been putting an antivirus on their computers, and I will say -- and I thought this was what you said earlier -- that an antivirus program is not going to identify a P2P program, because it's looking for viruses, which are small, malicious programs that

operate in the background that you don't know about, that you may get on your computer by what you just described, media that comes in with a link that says "Click on this link," you click on the link, and a program -- a virus program is downloaded onto your computer and operates in the background. But that's not what we're alleging here was the problem in this explanation.

What we're alleging here was the failure to have a penetration test would not identify to the company other risks that could not be identified by an antivirus program. That's why the IT professionals tell us that you really need to have a variety of tools to identify risks, because there's no one tool that will identify all the threats that a company faces.

JUDGE CHAPPELL: Okay. Now I follow why you're talking about antivirus. Go ahead.

MR. SHEER: The complaint alleges that LabMD did not use adequate measures, such as pen tests, to identify commonly known or reasonably foreseeable risks. As a result, it was blind to some risks and, therefore, unlikely to effectively guard against them.

To sum up, the complaint alleges that LabMD's security failures went beyond sharing a file with sensitive information about 9300 people to a P2P

network. The company's security practices created vulnerabilities an outsider could stitch together to find a way into the network, to move around the network and explore it, to find sensitive information, and then to package up the information and export it from the network without the company's noticing.

LabMD failed to implement reasonable security measures, and that is an unfair act or practice because it caused or is likely to cause substantial consumer injury that's not offset by countervailing benefits to consumers or competition and also not reasonably avoidable by consumers. After all, how can a consumer even know what LabMD's security practices were, let alone assess how adequate or inadequate they might be?

One final point. Neither the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward. They do not, for example, require that a certain vulnerability scanning product be used. Because security threats and responses change so rapidly, the order leaves it to the company to determine the particular security measures that, taken together, will provide reasonable security at lowest cost in its circumstances.

Although the Commission retains the right to do so, under the notice order and all of the other

21

Commission information security consent orders, a strong indication that security is reasonable is a security certification from an independent IT professional who's capable of balancing the costs and benefits and follows protocols commonly used in the profession. These are the same sorts of things that internal IT employees commonly do for companies across the country. Frankly, the order only asks LabMD to do what it should have been doing anyway but didn't.

Thank you.

JUDGE CHAPPELL: I have one question. I heard you refer to Section 5, but I also heard you refer to various other rules, regulations, et cetera. Is it the Government's position that whatever rule or regulation or statute that you're alleging was violated is contained within the four corners of this complaint?

MR. SHEER: What we're saying is that the allegation is that the company failed to comply with Section 5 in engaging an unfair act or practice by failing to provide reasonable security for sensitive information. We are saying 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 and

22

Technology, private entities, such as the SANS Institute, and many others as well. So that we are assessing reasonable -- reasonableness in much the same way, following the same process that is commonly used throughout the IT industry now. We add only one additional factor, and that is take into account the potential consumer harm from failing to have reasonable security to protect that information.

JUDGE CHAPPELL: I'm not sure you answered my question, Counselor. 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?

MR. SHEER: I misunderstood. I'm sorry. No.

JUDGE CHAPPELL: All right. Thank you.

MR. RUBINSTEIN: The facts in this case are pretty simple and pretty clear. The billing manager, the person responsible for handling LabMD's invoicing -- a small company, a very limited staff --

JUDGE CHAPPELL: Tell me more about what LabMD does. Do you take blood samples?

MR. RUBINSTEIN: It's a pathology lab. The customers -- LabMD's customers are doctors. You go in to see a doctor -- and it's a very small specialty business for particular kinds of cancer detection. You go in to see a doctor. He will take a tissue sample for

23

biopsy or what have you. They don't do the work in the lab, they send it out, and LabMD's market, which is primarily Georgia and the states surrounding it, it would do biopsies and give diagnoses to help with cancer treatment.

JUDGE CHAPPELL: So, that work is actually done in your company offices.

MR. RUBINSTEIN: That's correct.

JUDGE CHAPPELL: You have got the guys in the white lab coats.

MR. RUBINSTEIN: That's correct.

JUDGE CHAPPELL: Are you doing blood tests, like cholesterol?

MR. RUBINSTEIN: No. No, it's only -- and I don't want to speculate, and we will put this in obviously in the facts, but it's related to cancer diagnoses, but only certain kinds of cancers, prostate cancers, other sort of related maladies.

JUDGE CHAPPELL: So, generally a doctor takes a biopsy; they send it to you.

MR. RUBINSTEIN: That's correct.

JUDGE CHAPPELL: Okay.

MR. RUBINSTEIN: So, the doctors are our customers, technically.

JUDGE CHAPPELL: And the doctor sends the

24

patient data to you? Where does the data come from that's alleged to have been released in this case?

MR. RUBINSTEIN: The data came from an internal spreadsheet that was used by the billing manager, as I understand it -- as we understand it, to keep track of the accounts. She was in charge of making sure that the insurance companies got billed for the work that LabMD was doing. It was an internal spreadsheet. It was never meant to be shared with anybody.

And actually, I would like to, if I could, just take issue with the file that triggered this investigation was not shared; it was stolen. A company called Tiversa, under a government contract --

JUDGE CHAPPELL: Wait. I'd like to make sure I understand the particulars, to get a grasp of the big picture.

MR. RUBINSTEIN: Yes, sir.

JUDGE CHAPPELL: Somebody like INOVA Fairfax sends their tissue samples to your lab, and they probably have patient identifiable information on them, but then someone in your office developed a spreadsheet on their own, nothing to do with INOVA or Johns Hopkins or any other hospital. That was done internally, this spreadsheet.

MR. RUBINSTEIN: The spreadsheets were done

25

internally using information that came from the doctors.
JUDGE CHAPPELL: Right. But the doctors and the hospitals knew nothing about it.
MR. RUBINSTEIN: Well, I mean, I assume that they -- I don't know what they knew to begin with, but I'm going to assume they knew for billing purposes and invoicing we had to have some sort of billing procedures that --
JUDGE CHAPPELL: That's what I was going to ask you. Why was the spreadsheet created?
MR. RUBINSTEIN: To manage accounts, basically, accounts receivable.
JUDGE CHAPPELL: And that spreadsheet had personally identifiable information?
MR. RUBINSTEIN: Sure. It would identify the individual, their identifying number, and their insurance information, so that appropriate bills could be sent out.
JUDGE CHAPPELL: And did your client bill, for example, Blue Cross or did they bill the hospital or doctor who sent the sample?
MR. RUBINSTEIN: I think it differed from patient to patient depending on the particular circumstances, but I'm not 100 percent sure exactly, you know, what happened for each patient.

26

JUDGE CHAPPELL: It just -- you know, I find it helps to have a thorough understanding of the business to then go to an interpretation of what's going on and what -- and what has happened and what's not.
MR. RUBINSTEIN: Absolutely, Your Honor. It was standard kind of accounts receivable, is the best way to conceptualize what this spreadsheet was, and it was a way internally of tracking who it was and what was being paid and so forth.
And as I said, there are a couple of things here from a factual standpoint they are real simple and clear. The billing manager, she was in charge of -- as, you know, the proofs will show, she was in charge of managing money coming in, going out, and so forth, downloaded Limewire. Limewire is a P2P program that was primarily, I think, designed to share music and other files.
A government contractor by the time of Tiversa was paid, in conjunction with Professor Eric Johnson to surveil other companies --
JUDGE CHAPPELL: How do you spell that?
MR. RUBINSTEIN: Tiversa?
JUDGE CHAPPELL: Yes.
MR. RUBINSTEIN: T-I-V, Victor, E-R-S, as in Sam, -A.

27

JUDGE CHAPPELL: Is that like an incorporated company or --
MR. RUBINSTEIN: It's a security -- an internet security company based in Pittsburgh, a pretty large company. And apparently they had contracts with several government agencies to go out and see -- knock on doors, as if it were, and see if they could log in and steal files, and they did. And they put out a press release, Tiversa, that is --
JUDGE CHAPPELL: And just so you know, this is not argument. You are telling me what you're going to prove at trial.
MR. RUBINSTEIN: This is what's going to be proven, talking about right now the facts. They put out a press release claiming that they had found all sorts of breaches with spreadsheets that contained client names, Social Security numbers, birth dates, detailed hospital databases, over 20,000 patients, and the press release mentions the file that was taken from LabMD in this case.
The proofs will show that Tiversa notified the Respondent that it obtained one or stole one of LabMD's files --
JUDGE CHAPPELL: Let me make sure I understand this. You're saying Tiversa had a contract, they were

28

paid by our Government, to try to break in or hack files?
MR. RUBINSTEIN: Yes, sir. There was a study done by this Professor Eric Johnson in conjunction with Tiversa. I believe that the study was funded, according to Tiversa, by the Department of Homeland Security, among others. Yeah, it was designed to test the security of networks for confidential health and other information. And we will put into evidence --
JUDGE CHAPPELL: Are you aware of the details of that contract?
MR. RUBINSTEIN: We don't have a copy of the contract yet. We are going to get it in discovery we hope.
JUDGE CHAPPELL: For example, if you're a victim of the hacking, do they inform you and do they tell you what's been done?
MR. RUBINSTEIN: Well, that's what they did in this case, and then the testimony, certainly from LabMD's principals, is going to be that they then pitched their business. LabMD turned them down and said, "No, thank you," at which point in time the -- the stolen file made its way to the Government, and this proceeding followed.
So, we don't know at what point in time Tiversa

29

and the Government began communicating about LabMD. We anticipate that that relationship will be clarified in discovery, and it's obviously something we're very interested in.

JUDGE CHAPPELL: All right. You're saying you have proof, they told you you were hacked, they wanted to charge you to prevent attacks, but you're assuming they then spread the infor -- spread the data out.

MR. RUBINSTEIN: Well, as far as we know --

JUDGE CHAPPELL: Are you making a jump there or do you have proof of that?

MR. RUBINSTEIN: No, we believe -- we have proof of that. That's how the file came to the FTC, was from Tiversa. And, in fact, there will be testimony that a lawyer for Tiversa called a lawyer for LabMD, I think about a 12-, 13-month time frame, and said, "Well, we're giving this document now to the Government."

JUDGE CHAPPELL: Did you get any complaints from customers, your clients?

MR. RUBINSTEIN: No, sir. To the best of our knowledge, this file -- the only entities that have seen this, other than LabMD and its employees, are Tiversa and the Government.

JUDGE CHAPPELL: So, it's your position this information hasn't been released.

30

MR. RUBINSTEIN: That's correct. What we're also not clear, though, I should say, because this is -- as I mentioned, Tiversa puts out a press release identifying a number of other companies for which it attained data. It's not clear to us what happened to that data, where it went, whether it came to the Government, how the decision was made or why the decision was made to disclose LabMD's data. And, obviously, that -- all of those issues, we believe, are very significant and have very immediate, clear legal consequences. And so they are going to be addressed in discovery.

We also are, frankly, going to investigate why the Government knowingly commenced an investigation using a stolen file obtained from a government contractor being paid with taxpayer money to steal from LabMD. It doesn't make sense to us.

There are a number of very significant legal issues --

JUDGE CHAPPELL: Hold on a second.

Mr. Sheer, what's the Government's position on the disclosure of the data?

MR. SHEER: This comes down to a fundamental disagreement about how Limewire and other P2P applications work.

31

JUDGE CHAPPELL: Well, that's my job. I am going to deal with the fundamental disagreement.

MR. SHEER: Our view -- and we will put on evidence that shows this -- is that Limewire -- is that the LabMD file was not taken by being stolen; instead, Limewire does two things, basically two things. Someone installs it on their computer. It allows them to designate files on their computer that they will make freely available to anybody else on the Limewire network.

JUDGE CHAPPELL: I understand how P2P works. I may not look like it, but I understand technology.

MR. SHEER: Okay.

JUDGE CHAPPELL: What I want to know is what's your position of what happened to this actual data that's in dispute here or the subject of this dispute?

MR. SHEER: Our position is that the information was actually shared voluntarily from LabMD by virtue of its being in the "my shared files" folder in Limewire on the computer.

JUDGE CHAPPELL: And you have a witness who's going to say, "I saw it, they shared it with me"?

MR. SHEER: We have evidence that will show that the file that is in issue was, in fact, in the "my shared files" folder.

32

JUDGE CHAPPELL: That it was available to be viewed.

MR. SHEER: Correct. It was available to anyone who might look for it using Limewire.

JUDGE CHAPPELL: Kind of like when the Commission posted proprietary data a few years in a case that fortunately was not mine; there was this assumption that nobody had seen it, but now the assumption is somebody did see it?

MR. SHEER: Well, we know it was downloaded by one entity, they're saying Tiversa, and we also -- we also know that, because it was available, it could have been downloaded by any number of other people. And one would also want to say, even if you accept all of that -- which we don't -- it would have been very easy for the company to prevent this from having happened in the first place.

JUDGE CHAPPELL: And, again, I'm not -- clearly not making any substantive decisions today, but I'm just trying to figure out what the positions are, when I hear something this 180 degrees different. So, what you're telling me, though, is you're not going to have a witness say they saw it, but you intend to prove that it was available publicly.

MR. SHEER: We will be able to show that it was

33

available publicly and we may be able to have a witness who says they saw it.

JUDGE CHAPPELL: Do you have any complaining witnesses who say their data was released or disclosed?

MR. SHEER: Not at this time.

JUDGE CHAPPELL: Okay.

MR. SHEER: We will develop that.

JUDGE CHAPPELL: All right. Thank you.

MR. RUBINSTEIN: There are some very significant legal issues that are created by these facts. The first is the ambit of the Commission's authority under Section 5, which we intend to test. The second is the extent to which the file in question is within the Commission's ambit under Article 1, Section 8. There are due process issues, because notwithstanding counsel's discussions, there are no fixed or ascertainable standards by which LabMD, a small company, could judge the propriety of what it was doing.

Proofs will show that the billing manager downloaded Limewire and did it without the knowledge of the company's upper management and contrary to the company policy. This was not a shared file. This was not a shared file at all. It was never meant for public consumption. In fact, there's yet another issue here. LabMD is subject to HIPAA, and the Department of Health

34

and Human Services determined that no action was appropriate.

So, in effect, you have the Commission overfiling the agency of the Government that Congress designated with primary responsibility for management and regulation of HIPAA.

JUDGE CHAPPELL: So, you're saying -- your position is the data was not in a shared folder.

MR. RUBINSTEIN: It may have been in a -- it was in a folder and obviously it was accessible to Tiversa. The mechanics of how Tiversa accessed it and what kind of folder it was in are things that we are not clear about and we are going to, through discovery, better ascertain.

Certainly, it was not supposed to be made available to the public. That was not LabMD's policy, certainly, and to the extent that the Limewire was downloaded, it was done, as I said, without authorization and contrary to LabMD's standard policies.

JUDGE CHAPPELL: I've heard you say a couple times you're a small company. I mean, is that confidential? I mean, are you 5 million, 10 million? What kind of revenues? If it's not -- just ballpark. How small or how large are you.

MR. RUBINSTEIN: I would rather not -- I will

35

make that information available to you in camera.

JUDGE CHAPPELL: That's okay. I'll see it in the documents. I just thought, when you say small, you know --

MR. RUBINSTEIN: I would rather not -- we will say it is a small company with less than 50 employees, is my understanding. We will make that available to you, Your Honor.

JUDGE CHAPPELL: Less than 50, 5-0, or 15?

MR. RUBINSTEIN: I'm sorry, less than 50. But for various reasons, it's a closely held corporation, and I don't want to put the numbers out. But we are not INOVA or Johns Hopkins.

JUDGE CHAPPELL: Labcorp?

MR. RUBINSTEIN: Not them either.

So, what we anticipate with this case, as I said, we are going to have to find out Tiversa's role. We are going to have to find out the extent to which it was involved with and its relationship with the Commission in the decision to move forward with this investigation. And we're going to be filing a series of dispositive motions very early on, because quite frankly, we don't believe the Commission has the authority to be doing what it's doing to LabMD. We don't think that the information --

36

JUDGE CHAPPELL: Very early on?

MR. RUBINSTEIN: Very early on, within the -- I mentioned this to counsel. We anticipate filing a series of motions within the next two to three weeks.

JUDGE CHAPPELL: And you understand who will be deciding those motions?

MR. RUBINSTEIN: We are well aware, Your Honor, but we have an obligation to exhaust our remedies. So, we're going to be raising a series of legal issues. We're going to be raising a series of evidentiary objections based on the circumstances, as we understand them today, about how the Government came into possession of the information in the first instance.

And then all of the other things that are laid out in the complaint were the result of the knowing acceptance from a government contractor of a stolen file, files stolen, by the way, in contravention of Georgia's law. There was a case in the Eleventh Circuit which was dismissed for want of jurisdiction under the Georgia long arm statute, but there is, you know, a clear suggestion that what Tiversa did violate Georgia's law.

JUDGE CHAPPELL: Who brought that case?

MR. RUBINSTEIN: LabMD against Tiversa.

JUDGE CHAPPELL: And, of course, LabMD didn't

decide that motion, did they?
MR. RUBINSTEIN: Well, it was dismissed based on, like I said, lack of long arm jurisdiction. I have a copy of the Eleventh Circuit decision if you would like it. I can provide that to you right now, if you care to see it.
JUDGE CHAPPELL: It won't do me any good until after the hearing starts.
MR. RUBINSTEIN: But that's where we're at. We're going to be filing dispositive motions. We fully anticipate that the scope of discovery will be clarified. We look forward to working with the Government to ensure that this matter moves as quickly and as painlessly forward as possible. And we look forward to trying this issue before Your Honor.
JUDGE CHAPPELL: Anything else?
MR. RUBINSTEIN: I believe, for today, that's -- that's enough.
JUDGE CHAPPELL: I notice there's another attorney who's appeared in the case for your client. Are you -- can you let us know, is he going to be 50/50? Is he going to be involved in taking witnesses?
MR. RUBINSTEIN: Yes, Your Honor. And forgive me, I should have explained this up front. LabMD is represented by Cause of Action, a 501(C)(3) charity that

does government accountability, government watchdog, and government transparency work. In the interest of their educational mission, they from time to time take on lawsuits that implicate important issues. In this case, there's an organizational issue in the fact that you have a government commission acting and putting in jeopardy a small business without having any clear standards or ascertainable standards for doing so.
So, I'm a partner at Dinsmore & Shohl. I have a practice. Cause of Action is a client of mine from time to time. They asked me to serve as lead counsel. There will be a staff counsel from Cause of Action by the name of Michael Pepson who will be involved in this case. A lot of the document production and so forth that we will be doing will be coming from Cause of Action, but I will be serving as lead counsel and he will be assisting me.
JUDGE CHAPPELL: All right, thank you.
MR. RUBINSTEIN: Thank you.
JUDGE CHAPPELL: Mr. Sheer, anything further?
MR. SHEER: No, Your Honor.
JUDGE CHAPPELL: Okay. Hearing nothing further, we are, until we meet again, adjourned.
(Whereupon, at 2:46 p.m., the initial pretrial conference was adjourned.)

CERTIFICATION OF REPORTER
DOCKET/FILE NUMBER: DOCKET 9357
CASE TITLE: IN RE: LABMD, INC.
DATE: SEPTEMBER 25, 2013

I HEREBY CERTIFY that the transcript contained herein is a full and accurate transcript of the notes taken by me at the hearing on the above cause before the FEDERAL TRADE COMMISSION to the best of my knowledge and belief.

DATED: 9/25/2013

SUSANNE BERGLING, RMR-CRR-CLR

CERTIFICATION OF PROOFREADER

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

SARA J. VANCE, CMRS

A
able 11:3 12:16 32:25 33:1
Absolutely 26:5
accept 16:9 32:14
acceptance 36:16
access 8:22 14:18,25 15:7 17:22
accessed 34:11
accessible 34:10
accommodation 4:19
account 8:16 13:12 16:4 22:6
accountability 38:1
accounts 9:3 24:6 25:11,12 26:6
accuracy 39:21
accurate 39:7
achieve 16:21
act 9:10 10:14,21 11:4,10 20:8 21:19
acting 38:6
action 9:9 34:1 37:25 38:10,12,15
activities 17:13
actual 31:15
add 8:9 22:5
addition 9:23,25
additional 22:6
address 9:11
addressed 16:11 30:11
adequate 19:19 20:14
adequately 14:16,22
adjourned 38:22,24
Administrative 2:20
admittedly 16:10
afternoon 4:10,12
agencies 27:6
agency 34:4
ago 7:25 13:21
agreements 9:19
ahead 4:9 8:10 19:17
Alain 3:4 4:11
alarm 15:9
alerted 16:15
allegation 21:18
allege 22:11
alleged 24:2
alleges 11:3,15 15:14 19:18,23
alleging 19:7,9 21:15
allow 8:5
allows 15:17 31:7
ambit 33:11,14
AMERICA 2:1
amount 5:18
amounts 11:6
analyzing 13:9
answered 22:9
anticipate 5:19,21 6:23 29:2 35:16 36:3 37:11
antivirus 17:11,23 18:4,6,9,12,17,19 18:21,23 19:11,17
anybody 24:9 31:9
anyway 21:9
apparently 27:5
appearances 3:1 4:8
appeared 37:20
application 18:10
applications 17:20 30:25
Applying 14:11
appreciated 4:20
approach 11:18 13:9,11
appropriate 8:23 11:8 15:6 17:3 25:17 34:2
appropriately 14:17 14:20
approval 12:18
approximately 6:3 15:24
area 10:10,18
areas 9:12 11:2
argument 18:20 27:11
arm 36:20 37:3
Arthaud 3:25
Article 33:14
ascertain 34:14
ascertainable 33:16 38:8
asheer@ftc.gov 3:14
asked 38:11
asks 21:8
assess 20:14
assesses 9:22
assessing 22:3
assistant 5:10
assisting 38:16
associated 6:25
assume 25:4,6
assuming 29:7
assumption 32:7,8
attacks 29:7
attained 30:5
attorney 37:20
authenticate 14:21
authority 9:11 33:11 35:24
authorization 11:9 34:19
automated 17:12
available 13:1 14:1 15:18,20,22 21:23 31:9 32:1,3,12,24 33:1 34:16 35:1,7
Avenue 3:11,19
avoidable 11:13 20:12
aware 9:21 28:10 36:7

B
B 4:4
background 19:1,6
balance 13:16
balancing 13:1,2 21:4,22
ballpark 5:22 34:23
bank 9:3
based 27:4 36:11 37:2
basic 18:2
basically 10:2,16 17:19 25:11 31:6
basket 12:4
began 29:1
BEHALF 3:3,16
belief 39:10
believe 28:5 29:12 30:9 35:23 37:17
bells 15:9
benefit 13:16 21:22
benefits 9:5 11:14 13:1 20:10 21:4
Bergling 2:25 39:16
best 26:6 29:20 39:9
better 34:13
beyond 19:24
big 24:15
bill 25:19,20
billed 24:7
billing 15:16,17,19 16:17 22:16 24:4 25:6,7 26:12 33:19
bills 25:17
biopsies 23:4
biopsy 23:1,20
birth 15:25 27:17
blind 19:21
blood 8:12 22:20 23:12
Blue 25:20
body 7:13
boundaries 7:5
breaches 12:2 27:16
break 28:1
broad 9:11
brought 9:10 36:23
business 8:19,20 13:5 15:21,22 22:24 26:2 28:21 38:7
businesses 13:3

C
C 4:1 39:1,1,18,18
calculation 10:6
call 4:3 11:17
called 13:6 15:10,15 17:11,14 24:13 29:15
camera 35:1
cancer 22:24 23:4 23:16
cancers 23:17,18
capable 21:4
card 9:3
care 37:6
case 1:4 7:14 8:6 22:15 24:2 27:20 28:19 32:6 35:16 36:18,23 37:20 38:4,13 39:3
cases 13:8
cause 11:11 14:5 16:5 20:9 37:25 38:10,12,15 39:8
caused 20:9
causes 11:11
certain 10:19 20:18 23:17
certainly 28:19 34:15,17
certification 21:3
CERTIFY 39:6,20
cetera 21:13
change 12:16 20:20
CHAPPELL 2:19 4:3,7,14,21,24 5:3 6:1,4,9,13,16 7:1 8:3,5,18 9:13 10:8 10:17,21,23 16:23 18:4,11,15 19:16 21:11 22:9,14,19 23:6,9,12,19,22,25 24:14,18 25:2,9,13 25:19 26:1,21,23 27:1,10,24 28:10 28:15 29:5,10,18 29:24 30:20 31:1 31:11,14,21 32:1,5 32:18 33:3,6,8 34:7,20 35:2,9,14

36:1,5,23,25 37:7 37:16,19 38:17,19 38:21
charge 24:6 26:12 26:13 29:7
charity 37:25
checking 8:16
choir 18:14
cholesterol 23:13
Circuit 36:18 37:4
circumstances 11:20 20:23 25:24 36:11
claiming 27:15
clarified 29:2 37:12
classified 13:22
clear 22:16 26:12 30:2,5,10 34:12 36:21 38:7
clearly 32:18
click 19:4,4
clicked 18:13
clicking 18:11
client 25:19 27:16 37:20 38:10
clients 29:19
closely 35:11
CMRS 39:25
coats 23:10
codes 16:2,5
collected 8:14
collecting 11:5
come 4:22 24:1
comes 19:3 30:23
coming 26:14 38:15
commenced 30:14
comment 8:3
commission 2:2 3:3 3:9 4:11 7:13,18 7:20 9:11,14,18,21 9:24 10:3 11:3 20:24 21:1 32:6 34:3 35:20,23 38:6 39:9
Commission's 10:5 13:8,11 33:11,13
common 12:25 21:22,23
commonly 14:14 17:4 19:20 21:5,7 22:4
communicating 29:1
communications 5:9
companies 9:14 18:3 21:7 24:7 26:20 30:4
company 9:16,18 11:4 13:18 14:2,14 15:10 16:11 17:7 19:10,15 20:20 21:18 22:18 23:7 24:12 27:2,4,5 32:16 33:17,22 34:21 35:6
company's 12:6 13:5 15:5,16 17:14 20:1,6 33:21
competition 11:15 20:11
complaining 33:3
complaint 4:13 7:14 9:6 11:3,15 14:14 15:14 17:6 19:18 19:23 20:15 21:16 22:12 36:15
complaints 9:7 29:18
comply 21:18
comprehensive 15:1
computer 11:2 12:13 14:22 15:16 15:20 16:14 18:19 19:2,6 31:7,8,20
computers 12:14,16 12:17 15:12,12,18 17:20 18:22
concepts 13:17 14:11
conceptualize 26:7
conduct 9:2 16:3
conference 2:12 38:24
confidential 28:8 34:22
Congress 34:4
conjunction 26:19 28:4
connect 18:1
consent 9:19 21:1
consequences 30:11
Consider 13:17
considerable 14:5
consumer 6:7,12 10:6 11:6,12 13:12 13:19 14:6,8 15:7 20:9,12 22:7
consumers 8:13,15 8:24 11:13,14 15:24 20:11,12
consumption 33:24
contained 15:23 21:16 27:16 39:6
continuing 11:25
contract 24:13 27:25 28:11,13
contractor 26:18 30:16 36:16
contracts 27:5
contrary 33:21 34:19
contravention 36:17
control 12:13
controls 16:21
copies 5:5,6,12
copy 28:12 37:4
corners 21:16 22:12
corporation 2:7 35:11
correct 8:4 23:8,11 23:21 30:1 32:3
correctly 12:8 14:20
cost 13:16 14:6,9 20:23 21:22
costs 13:1 21:4
counsel 4:13,19 36:3 38:11,12,16
counsel's 33:15
Counselor 22:10
countervailing 11:14 20:10
country 21:7
couple 26:10 34:20
course 36:25
courtesy 5:5,6,11
covers 7:9
COX 3:6
cracks 17:15
created 18:5,7 20:1 25:10 33:10
credit 9:3
critical 13:23 14:4
Cross 25:20
current 7:1
customers 22:22,22 23:24 29:19

D

D 1:1 2:19 3:17 4:1 39:18
D.C 3:12,20
Dana 5:10
data 12:14 24:1,1,3 29:8 30:5,6,8,22 31:15 32:6 33:4 34:8
databases 27:18
DATE 39:4
DATED 39:12
dates 15:25 27:17
deadline 7:8
deal 5:1 31:2
decide 13:3 37:1
decided 7:20 18:17
deciding 10:4 36:6
decision 30:7,8 35:20 37:4
decisions 32:19
defense 11:17,18 12:25 14:12 16:21
defenses 17:14
degrees 32:21
Department 28:6 33:25
depending 9:1 25:23
depth 11:17,18 12:25 14:12 15:5 16:22
described 19:3
designate 5:8 31:8
designated 34:5
designed 26:16 28:7
detailed 27:17
details 28:10
detect 14:24 15:6
detected 16:14
detection 22:24
determine 20:21
determined 34:1
develop 7:3 9:12 33:7
developed 24:21
diagnoses 23:4,17
differed 25:22
difference 13:10,11
different 17:7 32:21
Dinsmore 3:18 38:9
directly 15:11
disagreement 30:24 31:2
disclose 30:8
disclosed 11:9 33:4
disclosing 13:5 14:4 16:4
disclosure 10:7 13:13 30:22
discovered 13:20 14:2
discovery 28:13 29:3 30:12 34:13 37:11
discussions 7:21,23 8:1 33:15
dismiss 7:15,18
dismissed 36:19 37:2
dispositive 7:7 35:22 37:10
dispute 31:16,16
Division 3:10
Docket 2:6 4:3 39:2
DOCKET/FILE 39:2
doctor 22:23,25 23:19,25 25:21

doctors 8:13 22:22 23:23 25:1,2
document 29:17 38:14
documents 35:3
doing 8:13 21:9 23:12 24:8 33:18 35:24,24 38:8,15
doors 27:6
downloaded 16:13 19:5 26:15 32:10 32:13 33:20 34:18
draft 5:14
due 33:14

E

E 1:1 4:1,1 39:1,1,1 39:18,18,18
E-R-S 26:24
earlier 18:23
early 35:22 36:1,2
easily 12:11 16:3,11
easy 13:15 32:15
economy 11:1
education 11:25
educational 9:24 38:3
effect 34:3
effectively 18:1 19:22
eggs 12:4
eight 5:24
either 6:18 35:15
Eleventh 36:18 37:4
email 5:5,9 18:12
employee 13:24 14:18
employees 12:20,23 14:16 21:6 29:22 35:6
engaged 11:4
engaging 21:19
ensure 37:13
entered 9:18
entities 22:1 29:21
entity 32:11
entry 12:9
equipment 13:4 14:23
Eric 26:19 28:4
ESQ 3:4,5,6,7,8,17
essential 10:25
et 21:13
evidence 28:9 31:4 31:23
evidentiary 7:17,19 36:10
exactly 18:8 25:24
example 9:1 12:6,15 13:6 20:18 25:20 28:15
exceeds 14:9
exception 10:5,5
excuse 16:17
exhaust 36:8
expect 4:21 5:24
expecting 6:11
experience 12:1
expert 6:21
experts 6:5,7,12,12
explained 37:24
explanation 19:8
exploit 12:8
explore 20:4
export 12:12 20:5
exposes 8:21
expressed 10:21
extent 33:12 34:17 35:18
extra 18:16

F

F 39:1,1,18,18,18
face 17:7
faces 19:15
fact 29:14 31:24 33:24 38:5
factor 22:6
facts 22:15 23:16 27:14 33:10
factual 26:11
fail 12:5
failed 11:16 14:14 15:2 20:7 21:18
failing 8:23 11:7 21:20 22:7
failure 15:5 17:2,3 19:9
failures 19:24
Fairfax 24:18
fairly 6:5
familiar 17:10
far 14:8 29:9
Federal 2:2 3:3,9 39:9
figure 32:20
file 6:25 7:10 15:8 15:22 19:24 24:11 27:19 28:23 29:13 29:21 30:15 31:5 31:24 33:13,22,23 36:17
file-sharing 15:9
filed 7:16,19
files 15:11,18,19,21 16:6,15 26:17 27:8 27:23 28:2 31:8,19 31:25 36:17
filing 35:21 36:3 37:10
final 12:24 20:15
finally 14:25
financial 9:1 10:15 10:20
find 12:11,12 20:3,4 26:1 35:17,18
firewall 12:7,7 17:17,18
firewalls 17:24
firms 9:20
first 5:13 8:7 12:3 14:1 15:5 16:18 32:17 33:10 36:13
fix 13:24
fixed 33:16
folder 31:19,25 34:8 34:10,12
follow 4:25 12:23 19:16
followed 28:24
following 10:4 13:17 22:4
follows 21:4
foreseeable 14:15 17:4 19:20
forgive 37:23
format 39:22
forth 26:9,14 38:14
fortunately 32:7
forward 20:17 35:20 37:12,14,15
found 27:15
foundational 18:2
four 21:16 22:12
frame 29:16
frankly 21:7 30:13 35:23
fraud 9:3 16:4
free 12:11 13:25 14:7 16:24 17:1
freely 31:9
Friday 5:16,16
front 37:24
FTC 9:6,10 10:17 29:13
full 39:7
fully 37:10
fundamental 30:23 31:2
funded 28:5
further 38:19,21

G

G 4:1
gain 12:9
Gebler 3:25
general 11:18
generally 11:17 23:19
Georgia 23:3 36:20
Georgia's 36:18,21
getting 5:19 12:17
give 5:11 23:4
given 11:1
giving 29:17
go 4:9 6:24,24 8:7 8:10 9:3 19:17 22:22,25 26:3 27:6
going 6:4,6 10:8 15:9 18:6,9,13,24 20:17 22:11 25:6,9 26:3,14 27:11,13 28:13,20 30:11,13 31:2,22 32:22 34:13 35:17,18,21 36:9,10 37:10,21 37:22
good 4:10,12 37:7
government 4:9,19 5:21 8:7 21:24 24:13 26:18 27:6 28:1,23 29:1,17,23 30:7,14,15 34:4 36:12,16 37:13 38:1,1,2,6
Government's 6:22 21:14 30:21
Gramm-Leach-Bl... 10:13
grasp 24:15
Gross 5:10
guard 19:22
guidance 10:2
guidelines 9:14
guiding 11:21 12:3
guys 23:9

H

hack 28:1
hacked 29:6
hacking 28:16
hand 14:6
handling 22:17
happened 15:7 16:8 25:25 26:4 30:5 31:15 32:16
hard 13:14
harm 6:24 10:7 13:12 14:6 22:7
harms 16:5
health 15:25 28:8 33:25
hear 6:10 32:20
heard 21:11,12 34:20

hearing 7:2,5,17,19 37:8 38:21 39:8
held 35:11
help 23:4
helps 26:2
high 14:3
highly 15:23
Hillary 3:25
HIPAA 33:25 34:6
history 5:13
Hold 30:20
holding 5:22
hole 18:5,18
holes 17:24
Homeland 28:6
Honor 4:6,10,12,16 4:23 6:6,14 8:4,11 10:24 26:5 35:8 36:7 37:15,23 38:20
HONORABLE 2:19
hope 28:14
Hopkins 24:22 35:13
hospital 24:23 25:20 27:18
hospitals 25:3
hour 13:24
hours 7:2
Human 34:1
hundreds 8:14,18 15:19
hyphenation 39:21
hypothetical 13:18 14:3

I

identifiable 24:20 25:14
identified 19:11
identify 14:14 17:3 17:6,24,25 18:1,9 18:24 19:10,13,14 19:20 25:15
identifying 11:19 12:24 17:8 25:16 30:4
identity 3:10 8:24 9:5,9 16:4
immediate 30:10
impersonate 8:25
implement 15:1 20:7,17
implicate 38:4
important 38:4
inadequate 20:14
inadvertently 16:7
incidents 12:21
includes 13:4 17:12
including 8:15 15:21,24 21:24
incorporated 27:1
increasing 11:1
independent 21:3
indicated 7:24
indication 21:2
individual 25:16
individuals 5:8
industry 9:25 10:1 11:21 13:7 22:5
infor 29:8
inform 28:16
information 8:14,16 8:21,25 9:1,2,4,8,9 9:15 10:7,25 11:7 11:8 12:12 13:13 14:15,18,25 15:1,3 15:7,23 16:3 17:5 17:22 19:25 20:4,5 21:1,21 22:8 24:20 25:1,14,17 28:9 29:25 31:17 35:1 35:25 36:13
initial 2:12 38:23
injury 6:8,12 11:12 11:13 20:10
INOVA 24:18,22 35:13
inside 17:19
install 12:17 14:7
installation 16:14
installed 15:15
installing 13:25 14:9
installs 31:7
instance 36:13
instances 13:15
Institute 11:24 21:25 22:2
institutions 10:15 10:20
insurance 9:4 16:1 24:7 25:17
intend 7:10 32:23 33:12
interest 7:24 38:2
interested 29:4
internal 21:6 24:3,8
internally 24:23 25:1 26:8
internet 27:3
interpretation 26:3
intruder 17:15
investigate 30:13
investigation 24:12 30:14 35:21
invoicing 22:17 25:7
involved 35:19 37:22 38:13
irony 16:9
issue 5:15 7:13 24:11 31:24 33:24 37:15 38:5
issued 9:14 10:1,9 10:12,13,14
issues 6:7,24 30:9,19 33:10,15 36:9 38:4

J

J 39:25
jeopardy 38:7
Jersey 3:11
job 12:15 31:1
jobs 14:19
Johns 24:22 35:13
Johnson 26:19 28:4
judge 2:20 4:3,7,14 4:21,24 5:3,23 6:1 6:4,9,13,16 7:1 8:3 8:5,18 9:13 10:8 10:17,21,23 16:23 18:4,11,15 19:16 21:11 22:9,14,19 23:6,9,12,19,22,25 24:14,18 25:2,9,13 25:19 26:1,21,23 27:1,10,24 28:10 28:15 29:5,10,18 29:24 30:20 31:1 31:11,14,21 32:1,5 32:18 33:3,6,8,17 34:7,20 35:2,9,14 36:1,5,23,25 37:7 37:16,19 38:17,19 38:21
judgment 7:9,10
judgments 7:12
jump 29:10
jurisdiction 10:17 10:19 36:19 37:3

K

keep 7:4 24:5
kind 16:2 26:6 32:5 34:11,23
kinds 11:19 22:24 23:17
knew 25:3,5,6
knock 27:6
know 7:11 8:8 18:18 19:1 20:13 25:5,25 26:1,13 27:10 28:25 29:9 31:14 32:10,12 35:4 36:20 37:21
knowing 36:15
knowingly 30:14
knowledge 29:21 33:20 39:9
known 11:22 14:14 16:19 17:4 19:20
knows 4:25

L

lab 22:21 23:2,10 24:19
Labcorp 35:14
LabMD 2:6 4:4,5 7:24 8:11,21 9:8 11:4,15 14:11 15:2 15:8,15 16:9,14 19:18 20:7,17 21:8 22:19 24:7 27:19 28:21 29:1,15,22 30:17 31:5,18 33:17,25 35:24 36:24,25 37:24 39:3
LabMD's 18:2 19:23 20:13 22:17 22:22 23:2 27:22 28:20 30:8 34:16 34:19
laboratory 8:12
lack 37:3
laid 36:14
large 11:6 27:4 34:24
LASSACK 3:7
latest 5:17
Laura 3:5 4:13
law 2:20 36:18,22
lawsuits 38:4
lawyer 29:15,15
lead 38:11,16
learned 12:1
leaves 20:20
legal 30:10,18 33:10 36:9
lessons 12:1
level 12:14
leveraged 17:22
Limewire 15:15,17 15:19,20 16:6,8,10 16:12,18,23 26:15 26:15 30:24 31:4,6 31:9,19 32:4 33:20 34:17
limit 5:18,20 8:6 12:13 14:17
limited 7:2 22:18
link 18:11 19:3,4,4
listed 5:4
little 4:22 15:4
LLP 3:18
log 27:7

long 7:25 36:20 37:3
look 9:16,18 11:3 31:12 32:4 37:12 37:14
looking 17:15,16,17 17:18,21 18:24
loss 13:5 14:3,8
lot 38:14
lots 11:22
low 14:7
lowest 12:14 20:22

M

maintaining 12:21
maintains 9:8
making 18:20 24:6 29:10 32:19
maladies 23:18
malicious 18:25
manage 25:11
management 13:6,7 13:17 33:21 34:5
manager 15:16,17 16:17 22:16 24:4 26:12 33:19
manager's 15:20
managing 26:14
MARGARET 3:7
market 23:2
materials 9:24 11:23
matter 2:5 37:13
mean 25:4 34:21,22
meant 24:9 33:23
measure 12:5,6
measures 8:24 11:8 11:19 12:10,19,24 13:2,10 14:24 15:3 15:6 16:21 17:3,9 19:19 20:8,21
mechanics 34:11
mechanism 7:3
media 19:3
medical 8:12,16 9:4 16:2,4
meet 38:22
MEGAN 3:6
MEHM 3:8
mentioned 30:3 36:3
mentions 27:19
method 9:21
methodology 10:3
Michael 2:19 38:13
microphone 6:10,17
microphones 6:17
middle 6:18
million 34:22,22
mine 32:7 38:10
minutes 8:7,9
mission 38:3
mistake 12:8
mistakes 16:19
misunderstood 22:13
misused 9:2,4 16:3
modifications 5:14
moment 8:1
money 26:14 30:16
monitor 5:23
motion 5:1 7:14,15 37:1
motions 4:25 7:7,9 7:18,19 35:22 36:4 36:6 37:10
move 6:5 20:3 35:20
moves 37:13
music 26:16

N

N 1:1 4:1 39:1,18
N.W 3:11,19
name 38:12
names 8:15 13:19 14:4 15:24 16:1 27:17
national 8:19,20 11:24 21:25
near 5:19
necessarily 18:15
need 4:25 5:7,21 6:9 7:3 12:15 16:9,10 19:13
needed 14:18 16:21 17:25 18:19
needs 6:10 12:14
negotiations 9:19
Neither 20:15
network 12:7,9,11 15:9,10,13 17:19 17:20 18:10 20:1,3 20:3,6 31:10
networks 11:2 18:1 28:8
never 8:22 24:9 33:23
new 3:11 9:2,12 11:2 13:4 16:3
nontechnical 12:19
Norton 18:12
notes 39:7
notice 5:3 20:16,25 37:19
noticing 20:6
notified 27:21
notwithstanding 33:15
number 6:3 9:6 10:1 14:13 25:16 30:4 30:18 32:13 39:2
numbers 8:16 13:19 14:5 15:25 16:1 27:17 35:12

O

O 4:1 39:1,1,1,18,18 39:18,18
OALJ 5:10
objections 36:11
objective 18:16
obligated 5:16
obligation 36:8
obtained 27:22 30:15
obviously 14:8 23:16 29:3 30:9 34:10
office 5:4,7,9,12 24:21
offices 23:7
Official 5:6
offset 11:14 20:10
okay 4:3,7,14 6:1,13 7:1 10:23 19:16 23:22 31:13 33:6 35:2 38:21
Once 17:19
ongoing 8:2
online 18:2
open 9:2 18:12
opening 17:18
operate 19:1
operates 19:6
operating 14:23
opportunity 4:18
order 4:3 5:14,15 7:7,8 20:16,20,25 21:8
orders 5:5 21:1
organizational 38:5
organizations 21:24 21:24
outside 17:15
outsider 12:8,10 20:2
overfiling 34:4
overview 1:4 8:6

P

P 4:1 39:1,18
p.m 2:14 38:23
P2P 15:11,14 18:5 18:10,17,24 19:25 26:15 30:24 31:11
package 20:5
PAGE 1:4
paid 26:9,19 28:1 30:16
painlessly 37:14
paragraph 14:13 15:14 17:5
part 10:25
particular 11:20 20:21 22:24 25:23
particulars 24:15
parties 4:8 5:5 7:3 7:25
partner 38:9
party 5:7
pass 14:11
pathology 22:21
patient 24:1,20 25:23,23,25
patients 27:18
pay 18:16
peer-to-peer 15:8 15:10
pen 17:13,16,24 19:19
penetration 17:12 19:10
Pennsylvania 3:19
people 5:4,11 8:22 15:12 16:19 19:25 32:13
Pepson 38:13
percent 25:24
perform 12:15
person 22:17
personal 8:24 9:8 14:15,25 17:5
personally 25:14
picture 24:16
pieces 10:2,2
pitched 28:21
Pittsburgh 27:4
place 12:10 16:18 32:17
plan 12:20
plans 13:6
point 7:25 18:7,8,8 18:16,18 20:15 28:22,25
policies 12:22 34:19
policy 16:1 33:22 34:16
position 21:14 29:24 30:21 31:15,17 34:8
positions 32:20
possession 36:13
possible 13:10,10 37:14
posted 32:6
potential 10:6 13:5

13:12 14:2,8 22:7
practical 11:25
practice 4:25 11:5 11:10,16 20:8 21:19 38:10
practices 9:12 14:17 20:1,13,16
preaching 18:14
preliminary 7:22
prescribes 20:16
present 3:24 8:6 16:6
presenting 6:21
press 27:8,15,18 30:3
pretrial 2:12 38:23
pretty 22:16,16 27:4
prevent 11:8 14:24 15:6 29:7 32:16
prevented 16:13
primarily 23:3 26:16
primary 34:5
principals 28:20
principles 11:21,23 12:3
prior 12:18
privacy 3:10 16:5
private 22:1
probably 24:20
probe 17:14
problem 19:7
procedures 12:22 25:7
proceeding 28:24
process 10:6 13:2 22:4 33:14
product 20:19
production 38:14
profession 21:5
professional 14:7 21:3
professionals 11:16 11:21,25 13:7,21 17:8 19:12
Professor 26:19 28:4
program 13:18,20 15:1,15 17:11 18:5 18:9,10,23,24 19:5 19:5,12 26:15
programs 12:17 16:19 17:21,23 18:25
proof 29:6,11,12
proofread 39:20
proofs 26:13 27:21 33:19
proprietary 32:6
propriety 33:17
prostate 23:17
protect 9:15 15:3 22:8
Protection 3:10
protocols 21:5
prove 27:12 32:23
proven 27:14
provide 7:15 12:25 20:22 21:20 37:5
provided 9:25
provider 16:1
provides 9:11
providing 12:20
public 2:15 9:23 13:21 33:23 34:16
publicized 12:1
publicly 32:24 33:1
published 11:23
punctuation 39:21
purchase 13:4
purchased 16:24
purposes 25:6
pursue 7:25
put 7:8 12:4 18:19 23:15 27:8,14 28:9 31:3 35:12
puts 30:3
putting 5:24 18:21 38:6

Q

qualitatively 13:16
question 21:11 22:10 33:13
questions 8:8
quickly 6:5 37:13
quite 35:22
quote 11:17

R

R 4:1 39:1,1,1,1,18 39:18,18,18
raising 36:9,10
rapidly 20:20
reads 10:15
real 26:11
really 19:13
reasonable 8:23 11:7,20 12:25 14:24 15:2 20:7,22 21:2,20 22:3,7
reasonableness 9:22 10:4 13:9 21:21 22:3
reasonably 11:13 14:15 17:4 19:20 20:11
reasons 35:11
rebuttal 6:22
receivable 25:12 26:6
receive 5:8,11
received 9:7
Reed 3:17 4:16
reed.rubinstein@... 3:22
refer 21:12,12
regard 9:13 10:13
regarding 7:6,6
regulation 21:14 34:6
regulations 21:13 22:10
reign 12:11
related 17:13 23:16 23:18
relationship 29:2 35:19
relatively 13:15
release 27:8,15,19 30:3
released 24:2 29:25 33:4
reliance 11:1
remedies 36:8
Reported 2:25
represented 37:25
representing 4:11 4:17
request 4:22
require 20:18
requires 17:9
respect 7:14
Respondent 3:16 4:15,17 6:2 7:23 27:22
responding 12:21
responses 20:19
responsibility 34:5
responsible 22:17
result 19:21 36:15
results 8:17
retains 20:24
revenues 34:23
right 20:24 22:14 25:2 27:14 29:5 33:8 37:5 38:17
RIPOSO 3:5
risk 13:6,16,22,23 16:6,9,11
risks 14:15,17 17:4 17:8 18:1 19:11,14 19:20,21
RMR-CRR-CLR 2:25 39:16
role 35:17
Rubinstein 1:6 3:17 4:6,16,16,23 5:2 6:3,14,19 8:4 22:15,21 23:8,11 23:14,21,23 24:3 24:17,25 25:4,11 25:15,22 26:5,22 26:24 27:3,13 28:3 28:12,18 29:9,12 29:20 30:1 33:9 34:9,25 35:5,10,15 36:2,7,24 37:2,9 37:17,23 38:18
rule 7:9 10:13,14,15 21:14
ruled 7:12,17
rulemaking 10:8,12
rules 5:17 7:1,15 10:9,12 21:13 22:10
RYAN 3:8

S

S 4:1
safeguards 10:14
Sam 26:25
sample 22:25 25:21
samples 8:12 22:20 24:19
SANS 22:1
SARA 39:25
saw 31:22 32:23 33:2
saying 8:19 10:24 21:17,21 27:25 29:5 32:11 34:7
says 19:3 33:2
scale 13:22
scan 17:13
scanning 20:18
schedule 4:20
scheduling 5:14 7:6 7:8
scope 37:11
second 12:13 17:2 30:20 33:12
Secretary 5:7
Section 9:10,10 11:5 21:12,19 33:11,14
security 8:15,23 10:25 11:8,19 12:5 12:6,10,16,20,21 12:22 13:2,9,19 14:5,16 15:1,3,25 16:20 17:7 19:24 20:1,7,13,16,19,21 20:22 21:1,2,2,20 22:8 27:3,4,17 28:6,8

see 7:4 22:23,25 27:6,7 32:9 35:2 37:6
seen 29:21 32:8
select 15:18
send 5:9 23:2,20
sends 23:25 24:19
sense 12:25 21:22,23 30:17
sensitive 8:14 11:6 12:12 15:3,23 17:22 19:25 20:4 21:20
sent 25:18,21
SEPTEMBER 2:13 39:4
series 9:20 35:21 36:4,9,10
serve 38:11
service 5:6
Services 34:1
serving 38:16
SESSION 2:15
set 9:19 10:2 11:10 12:7 13:8 14:13 17:5
sets 11:20
settings 12:16
settlement 7:21,23 7:24 8:1
seven 5:24
share 15:11 26:16
shared 15:8,22 16:7 16:7,15 24:9,12 31:18,19,22,25 33:22,23 34:8
sharing 16:16 19:24
Sheer 1:5 3:4 4:10 4:11 5:23 6:6,11 7:22 8:11,20 9:17 10:11,19,22,24 16:25 18:8,14,20 19:18 21:17 22:13 30:21,23 31:3,13 31:17,23 32:3,10 32:25 33:5,7 38:19 38:20
Shohl 3:18 38:9
show 26:13 27:21 31:23 32:25 33:19
shows 31:4
side 5:4 8:5
significant 30:10,18 33:9
similar 13:3
simple 22:16 26:11
single 12:4 17:6
sir 24:17 28:3 29:20
site 5:10
Sloane 3:25
small 18:25 22:18 22:23 33:17 34:21 34:24 35:3,6 38:7
Social 8:15 13:19 14:5 15:25 27:17
software 18:17,17
somebody 24:18 32:9
sooner 4:22
sorry 6:11 22:13 35:10
sort 23:18 25:7
sorts 21:6 27:15
sources 11:23 21:23
space 4:4
speak 6:10
specialty 22:23
specific 20:16
speculate 23:15
spell 26:21
spelling 39:21
spread 29:8,8
spreadsheet 24:4,8 24:21,24 25:10,13 26:7
spreadsheets 24:25 27:16
staff 22:18 38:12
stand 6:9,17
standard 26:6 34:19
standardized 16:2
standards 11:24 21:25 33:16 38:8,8
standpoint 26:11
start 4:8,9 7:16,19
starts 37:8
statements 9:23
states 2:1 23:3
statute 21:15 36:20
steal 9:4 27:7 30:16
step 12:24
stitch 20:2
stole 27:22
stolen 24:12 28:23 30:15 31:5 36:16 36:17
stop 16:16 18:6,13
stopped 16:12
store 13:18
storing 11:6
stretching 7:4
strong 21:1
study 28:3,5
subject 31:16 33:25
substantial 11:12 20:9
substantive 7:15,18 32:19
suggestion 36:21
Suite 3:19
sum 19:23
summary 7:8,10,12
supposed 34:15
sure 22:9 24:6,14 25:15,24 27:24
surrounding 23:3
surveil 26:20
Susanne 2:25 39:16
system 7:3
systematically 11:16 15:2
systems 14:23

T

T 39:1,1,1,18,18
T-I-V 26:24
table 8:2
take 4:18 8:9,13,23 14:23 22:6,20,25 24:11 38:3
taken 20:21 27:19 31:5 39:8
takes 13:11 23:19
talk 7:7 15:4
talking 18:4 19:17 27:14
taxpayer 30:16
technical 6:7,12,24 16:20
technically 23:24
technology 11:24 22:1 31:12
tell 7:11 17:8 19:12 22:19 28:16
telling 18:19 27:11 32:22
ten 9:5
test 8:16 17:12,16 17:17,20,20 19:10 28:7 33:12
testimony 6:21,22 28:19 29:14
tests 8:12 17:13,24 19:19 23:12
thank 4:7,18,18 5:2 8:11 21:10 22:14 28:22 33:8 38:17 38:18
thanks 5:14
theft 6:25 9:5 16:4
thieves 8:24 9:9
thing 7:6
things 21:6 26:10 31:6,6 34:12 36:14
think 5:13,16 25:22 26:16 29:15 35:25
thinking 6:4
Third 12:19
thorough 26:2
thought 18:22 35:3
thousands 8:15,18 13:19
threats 17:7 19:15 20:19
three 6:23 36:4
time 4:22 5:13,18 8:5,9 10:9 13:21 26:18 28:22,25 29:16 33:5 38:3,3 38:10,11
times 34:21
tissue 8:12 22:25 24:19
TITLE 39:3
Tiversa 24:13 26:18 26:22 27:9,21,25 28:5,6,25 29:14,15 29:22 30:3 32:11 34:10,11 36:21,24
Tiversa's 35:17
today 32:19 36:12 37:17
told 17:23 29:6
tomorrow 5:15
tool 17:6,10,11 19:14
tools 17:9 18:2 19:13
track 7:4 24:5
tracking 26:8
Trade 2:2 3:3,9 39:9
train 14:16
training 12:20
transcript 39:6,7,20
transparency 38:2
treasure 8:21
treatment 16:2,5 23:5
tremendous 10:1
trial 5:19 27:12
triggered 24:11
trove 8:21
try 28:1
trying 32:20 37:15
turn 17:2
turned 28:21
two 5:4,8,11 6:23 15:4 31:6,6 36:4
types 10:20

U

unauthorized 10:7 13:12 14:24 15:6
understand 24:5,5 24:15 27:24 31:11

31:12 36:5,11
understanding 16:25 26:2 35:7
unfair 11:4,11 20:8 21:19
UNITED 2:1
unquote 11:17
unreasonable 14:10
update 13:25 14:7,9 14:22
upper 33:21
USC 11:10
use 6:10,11,16,17 8:24 11:1,7 12:19 15:2,5 16:19 17:3 18:17 19:19
user 12:14
user's 12:13
users 12:15 14:21 15:11,17,19 16:8
uses 13:18
usually 17:8,12
utilize 9:15

V

VANCE 39:25
VanDruff 3:5 4:12 4:13
variety 8:25 17:9 19:13
various 21:13 35:11
verify 14:21
victim 28:15
Victor 26:24
Victoria 3:25
view 31:3
viewed 32:2
violate 36:21
violated 21:15 22:11
violation 11:5
virtue 31:18
virus 19:5
viruses 17:25 18:25
voluntarily 31:18
voted 7:13
vulnerabilities 9:20 17:21 20:2
vulnerability 13:20 13:22,25 14:1,4 17:13,17,18 20:18
vulnerable 12:5

W

Wait 24:14
want 5:11 9:9 23:15 31:14 32:14 35:12 36:19
wanted 29:6
Washington 3:12,20
watchdog 38:1
watching 5:23
way 10:15,16 14:12 20:3 22:4 26:6,8 28:23 36:17
ways 8:25 14:13
we're 5:18,20 18:20 19:7,9 21:17 29:3 29:16 30:1 35:21 36:9,10 37:9,10
Web 5:10
weeks 36:4
welcome 4:21
went 19:24 30:6
white 23:10
witness 31:21 32:23 33:1
witnesses 5:20,25 6:22 33:4 37:22
word 4:5,6
work 23:1,6 24:7 30:25 38:2
working 37:12
works 6:19,19 10:16 31:11
written 12:22

X

X 1:1

Y

Yeah 28:7
year 13:21
years 9:5 11:22 18:3 32:6

Z

0

1

1 13:23 33:14
10 13:22,23,23 14:13 17:5 34:22
100 25:24
101 14:12
12 29:16
13-month 29:16
15 8:7,9 11:10 35:9
18 15:14
180 32:21

2

2:00 2:14
2:46 38:23
20,000 27:18
20001 3:12
20004 3:20
2012 9:7
2013 2:13 39:4
202 3:13,21
210 7:2
22 1:6
25 2:13 39:4

3

326-2999 3:13
369,000 9:7
372-9100 3:21

4

45(n) 11:10

5

5 9:10,10 11:5 21:12 21:19 33:12 34:22
5-0 35:9
50 35:6,9,10
50/50 37:21
501(C)(3) 37:25
57 9:19

6

601 3:11
610 3:19

7

8

8 1:5 33:14
801 3:19

9

9/25/2013 39:12
9300 15:24 19:25
9357 2:6 4:4 39:2

EXHIBIT 10

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 11

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**
	)	**PUBLIC**
LabMD, Inc.,	)	
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

INTRODUCTION 1

STATEMENT OF FACTS 4

STANDARD OF REVIEW 8

ARGUMENT 9

I. The Commission Lacks Section 5 "Unfairness" Authority to Regulate Patient-Information Data-Security Practices. 9

A. Congress Authorized HHS, Not The FTC, To Regulate Patient-Information Data-Security Practices. 10

1. Controlling interpretative canons hold the FTC's general Section 5 authority (if any) must yield to the specific patient-information statutes and regulations. 10

2. The *Billing* doctrine controls and so the FTC has no authority. 13

B. Congress Has Not Given The FTC The Plenary Power To Regulate Data-Security Through Its Section 5 "Unfairness" Authority. 14

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. 14

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. 16

C. *ABA v. FTC* Stands For Dismissal. 20

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 22

A. Due Process Requires Fair *Ex Ante* Warning of Prohibited or Required Conduct. 22

B. The Commission Has Denied LabMD Fair Notice 23

1. The Commission has wrongfully failed to provide *ex ante* notice through regulations. 23

2. The FTC's alleged "standards" are legally meaningless. 24

III. The Acts or Practices Alleged in the Complaint Do Not Affect Interstate Commerce. 28

IV. The Complaint Does Not Comply with the Commission's Pleading Requirements. 28

V. This Matter Should Be Stayed Pending Disposition of this Motion 29

CONCLUSION 30

PUBLIC

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. The FTC's alleged "standards" are legally meaningless.

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

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., 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 12

FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
12 02 2013
567574
SECRETARY

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.	)	
	)	

RESPONDENT LabMD, INC.'S REPLY TO COMPLAINT COUNSEL'S RESPONSE IN OPPOSITION TO RESPONDENT'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
Senior Vice President for Litigation and Counsel to Cause of Action.

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.

INTRODUCTION

FTC's Opposition to LabMD's Motion is remarkable in only two respects. First, it demonstrates FTC has discarded rule-of-law and constitutional values for boundless bureaucratic power and discretion. Second, it shows FTC will distort the law and even re-write history to justify its power-grab.

FTC's Opposition's admissions and arguments demonstrate only that FTC lacks Section 5 authority over patient-information data-security, and that its standardless, blame-the-victim *ex post* enforcement tactics violate due process and fail to provide LabMD with constitutionally-adequate fair warning of the data-security standards FTC believes Section 5 forbids or requires.

STANDARD OF REVIEW

FTC does not respond to many arguments made in LabMD's Motion to Dismiss (Mot.). "[F]ailure to respond to an argument…acts as a concession" and thus an admission. *CREW v. Cheney*, 593 F. Supp. 2d 194, 229 (D.D.C. 2009).

FTC admits it must prove Congress intended to delegate it specific authority to regulate patient-information data-security. *La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986). FTC also admits the FRCP 12(b)(6) standard controls here under *In re S.C. State. Bd. of Dentistry*, 138 F.T.C. 229, 232 (F.T.C. 2004). *See* FTC Opp. to Mot. (Opp.) 3. Yet FTC claims without citing any controlling (or on-point) authority that the *Iqbal/Twombly* standard for 12(b)(6) motions does not apply. Opp. 25. Because FRCP 12(b)(6) applies here, as FTC admits, *Iqbal/Twombly* apply as well. *See Jones v. Horne*, 634 F.3d 588, 595-96 & n.4 (D.C. Cir. 2011)(*Iqbal/Twombly* sets standard for 12(b)(6) motions).

ARGUMENT

I. FTC LACKS SECTION 5 "UNFAIRNESS" AUTHORITY OVER DATA-SECURITY.

A. HIPAA/HITECH Control, And FTC May Not Over-File.

Citing no controlling authority or explicit statutory command, FTC wrongly claims "concurrent" jurisdiction over HIPAA/HITECH patient-information data-security.

FTC admits LabMD is and always has been a HIPAA-covered entity regulated exclusively by HHS under HIPAA/HITECH.[1] It also admits LabMD is specifically exempted from FTC's HITECH rule. *Cf.* Mot. 12 & n.9. It offers no explanation why HITECH, Pub. L. 111-5 §13424(b)(1), directs HHS and FTC to determine *which* agency is best equipped to enforce HITECH against non-HIPAA-covered entities (FTC agrees that HHS exclusively regulates HIPAA-covered entities like LabMD). It also ignores HIPAA's directive to HHS—not FTC—to "adopt [data-]security standards" for "health information." 42 U.S.C. §1320d-2(d)(1); 42 U.S.C. §1320d(4)(defining "health information").

Even if Section 5 covered data-security, HIPAA/HITECH are "precisely drawn, detailed statute[s that] pre-empt" Section 5's "more general remedies." *EC Term of Years Trust v. U.S.*, 550 U.S. 429, 433 (2007). Through HIPAA/HITECH, Congress deliberately targeted specific data-security problems with specific solutions, and these specific statutes govern over whatever "general" Section 5 authority FTC might have. *See RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 132 S. Ct. 2065, 2070-72 (2012). Otherwise, HIPAA-covered companies like LabMD lack data-security safe-harbor and certainty, contrary to HHS's regulatory intent.

[1] FTC incorrectly claims LabMD only cites one HITECH provision to support its argument. But LabMD cites multiple HIPAA provisions. Mot. 11-13 & nn.4,9.

See 78 Fed. Reg. 5,566, 5,644 (Jan. 25, 2013)(encouraging covered entities to use encryption safe-harbor); 65 Fed. Reg. 82,462, 82,543 (Dec. 28, 2000)(discussing safe-harbor).

FTC says "Congress's intent to preempt or repeal…FTC's unfairness authority" must be clear-and-manifest. Opp. 6. This distorts the law, for implied repeal may be found even "absent 'a clearly expressed congressional intention'" where, as here, two statutes irreconcilably conflict. *Carcieri v. Salazar*, 555 U.S. 379, 395 (2009).

FTC attempts to avoid *Credit Suisse v. Billing*, 551 U.S. 264 (2007), with the specious argument that the Court explicitly limited the rule there to conflicts between antitrust and securities laws. Opp. 7. But nowhere in *Billing* does it say this.[2] Instead, *Billing* fleshes out the analysis for determining a "clear repugnancy." *Billing* confirms that HIPAA/HITECH irreconcilably conflict with Section 5, and, being more recent and more specific than Section 5, control. *See Billing*, 551 U.S. at 276, 285. Even if the canon against implied repeal is applied here, Section 5 is displaced by HIPAA/HITECH. *See EC Trust*, 550 U.S. at 434-36.

FTC claims that because HITECH was enacted "*after*…[FTC] had brought a half-dozen unfairness cases relating to data security," Congress has blessed its power-grab. Opp. 7 n.4. That, too, distorts the law. Congress's failure to express any opinion is not probative of legislative intent. *Rapanos v. U.S.*, 547 U.S. 715, 749-50 (2006).

Finally, FTC's reliance on *two recent consent orders* in cases also involving allegations of Section 5 "deception" and HIPAA violations is another irrelevant distraction.[3] Here, the question is not whether Section 5 and HIPAA/HITECH authorities might be "complementary"

---

[2] *See* Jesse Markham, *The Supreme Court's New Implied Repeal Doctrine*, 45 GONZ. L. REV. 437,475 (2009)(*Billing* "not limited to…interplay between antitrust law and economic regulation.").

[3] *In re CVS Caremark* "is the first instance in which [HHS] OCR…coordinated …with…FTC." http://www.hhs.gov/news/press/2009pres/02/20090218a.html.

under some circumstances. Instead, it is whether FTC's "unfairness" authority allows FTC to over-file HHS and punish a company FTC admits *complied* with HIPAA/HITECH in all respects. FTC's interpretation of Section 5 wrongly eviscerates Congress's HIPAA/HITECH enactments and HHS's regulatory scheme.

B. FTC Lacks "Unfairness" Authority Over Data-Security.

FTC says its position that "companies *should* engage in 'reasonable' [data-security] practices…is premised on Congress's mandate" in 15 U.S.C. §45(n). Opp. 2 (emphasis added). This claim, yet again, distorts the law. Congress's subsection (n) mandate was to rein in FTC's abuse of its "unfairness" authority by, *inter alia*, prohibiting FTC from using public-policy considerations "as a primary basis for…determin[ing]" that a practice is "unfair." 15 U.S.C. §45(n).

1. Distorted History And Law Cannot Give FTC Data-Security Authority.

FTC distorts the legislative history to serve its power-grab. *See* Opp. 9. It cites "unfair-*competition*" materials from 1914 predating by twenty-four years the 1938 Wheeler-Lea Amendments to the FTC Act, which added "unfair or deceptive acts or practices" to Section 5, and predating by eighty years the 1994 Amendments, which added 15 U.S.C. §45(n). Therefore, FTC's alleged "legislative history" is irrelevant to its Section 5 "unfairness" authority here.[4]

FTC's case authority illustrates only that FTC lacks jurisdiction here. First, none of their cases are legally controlling. FTC admits that no court has ever affirmed its Section 5 authority

[4] FTC cites dicta from *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233 (1972), interpreting legislative history from the 1914 pre-Wheeler-Lea Amendments version of Section 5. But Congress was aware of this when it limited FTC's "unfairness" authority in 1994 in 15 U.S.C. §45(n) and overruled FTC's "unfairness" authority claims. *See Miles v. Apex Marine*, 498 U.S. 19, 32 (1990)("Congress…aware of existing law when it passes legislation"). Because *Sperry* was decided over twenty years before §45(n) was enacted, it is irrelevant.

to regulate patient-information or any other data-security. *Cf.* Mot. 1. Second, none of the cases cited are even factually analogous.

Unlike this case, where LabMD's property was taken by a third party without its knowledge or permission, in *FTC v. Neovi*, the defendant affirmatively participated in fraudulent creation and delivery of unverified checks. *See* 604 F.3d 1150, 1155-57 (9th Cir. 2010). Similarly, in *FTC v. Accusearch*, Accusearch was held liable for maintaining a website selling GPS locations of individual cell phones and other confidential, personal information, where every time Accusearch ordered phone records, they caused use of false pretenses and other fraudulent means to obtain this information. *See* 2007 U.S. Dist. LEXIS 74905, at *17-18 (D.Wyo. Sept. 28, 2007).

Unlike this case, where FTC admits LabMD has always complied with all applicable data-security regulations, *cf.* Mot. at 4,8,13, *Orkin Exterminating Co. v. FTC*—decided years *before* 15 U.S.C. §45(n)'s enactment limiting FTC's "unfairness" authority—involved unilateral breaches of unambiguous contracts through which Orkin wrongfully obtained money from consumers. *See* 849 F.2d 1354, 1363-66 (11th Cir. 1988).

Unlike this case, where FTC admits LabMD has not engaged in any deception, *cf.* Mot. 6, in *FTC v. Verity Int'l, Ltd.*, the defendant not only told its customers they were liable for payments for services they did not use or agree to but "misrepresented…services provided." 335 F. Supp. 2d 479, 484 (S.D.N.Y. 2004).

In re Int'l Harvester Co., 104 F.T.C. 949, 1984 FTC LEXIS 2 (1984), is a Commission decision predating Congress's attempt to rein in FTC via 15 U.S.C. §45(n). It is also factually inapposite. The "unfair" trade practice in that case was a deceptive material omission, i.e., the

company's failure to warn its customers about serious safety risks associated with its products. *Int'l Harvester*, 1984 FTC LEXIS at *255-62.

2. Congress's Preference for Sector-Specific Data-Security Statutes Trumps the Commission's Data-Security Power-Grab.

FTC again distorts the law, arguing FCRA, GLBA, and COPPA simply provide new "tools," such as "APA rulemaking authority…." Opp. 10. But Section 5 already gives FTC authority to promulgate rules. 15 U.S.C. §57a(a)(1). It just refuses to do so.

FTC also says LabMD "does not grasp the significance of civil penalties" and that under Section 5 FTC can seek only equitable relief. Opp. 11 (citing 15 U.S.C. §45(b)). Yet Section 5 authorizes civil penalties for cease-and-desist order violations of up to $10,000-per-violation, 15 U.S.C. §45(l), *and* authorizes substantial civil penalties for violations of "rules" respecting unfair acts or practices,[5] 15 U.S.C. §45(m).

Finally, FTC says FCRA, GLBA, and COPPA "enhance" FTC's general data-security authority because it need not prove a likelihood of substantial injury thereunder. Opp. 11. But if FTC actually issued data-security rules, as it is both authorized and constitutionally-required to do if Section 5 covered data-security, *see* 15 U.S.C. §57a(a), it would not need to prove substantial injury, 15 U.S.C. §45(m), and would have the same enforcement powers as it does under FCRA, GLBA, and COPPA, thereby rendering these statutes nullities. However, Congress recognized that FTC has no general Section 5 "unfairness" data-security authority and thus enacted these sector-specific statutes. FTC's "enhancement" argument therefore fails.

[5] Civil penalties under subsections (l) and (m) are *four times* higher than those available under the FCRA, 15 U.S.C. §1681s(a)(2)(A); COPPA incorporates FTC Act penalties, 15 U.S.C. §6505(d); and GLBA is enforced under the FTC Act, 15 U.S.C. §6805(a)(7). Thus, the monetary penalty in *U.S. v. Choicepoint*, No. 06-0198 (N.D.Ga. Feb. 15, 2006), was issued "pursuant to…Section(m)(1)(A) of the FTC Act." Stip. Final Judgment 4. Likewise, the Consent Decree in *U.S. v. Path*, No. 13-0448, ¶18 (N.D.Cal. Feb. 8, 2013), expressly states that the civil penalties are imposed "pursuant to Section 5(m)(1)(A) of the FTC Act…."

C. FTC Disclaimed Authority to Regulate.

Complaint Counsel says "FTC has consistently maintained its ["unfairness" data-security] authority" and that "[a] contrary conclusion requires…tortured application" of a Supreme Court case involving a different agency. Opp. 12. As a matter of fact, this claim straddles the line between distortion and outright deception. As a matter of law, this is breathtakingly wrong.

1. Against the Backdrop of FTC's Admitted Lack of Authority, Congress Enacted Numerous Targeted Data-Security Statutes.

FTC claims that "[s]ince 2000, the FTC has brought nearly fifty data-security cases, more than eighteen of which alleged…unreasonable security is an unfair…practice," citing a string of consent orders. Opp. 12 & n.9. But the *earliest* consent order they cite is dated "Sept. 20, 2005." Opp. 12 n.9. The earliest Commission statements they cite are dated "Mar. 21, 2007" and "Sept. 22, 2004," respectively. Opp. 13 & n.10. Even taking FTC's citations at face value, their world seemingly was created in late 2004.

Furthermore, FTC's out-of-context cherry-picked statement from a footnote in Orson Swindle's testimony must be addressed. *See* Opp. 13 n.10. He never suggested that the Commission has general substantive data-security authority under Section 5, for the very next sentence in footnote 24 states: "[FTC] has used this ["unfairness"] authority in appropriate cases to challenge a variety of injurious practices, including unauthorized charges in connection with 'phishing'" and cites two "phishing" cases.

Complaint Counsel does not mention FTC's statement in *Privacy Online: A Report to Congress*, 41 (1998), that FTC generally "lacks authority to require firms to adopt information practice policies," or its statement in *Privacy Online: Fair Information Practices in the Electronic Marketplace,* 34 (2000), that FTC "lacks authority to require firms to adopt

information practice policies or…abide by…fair information practice principles on their Websites" not directed to children. *Cf.* Mot. 16 n.12. They do not deny that Chairman Pitofsky told Congress the FTC's data-security authority is "limited…to ensuring…Websites follow their stated information practices." Mot. 16 n.12. They offer no response to a FTC official's 2001 statement that "'[t]he agency's jurisdiction is (over) deception….If a practice isn't deceptive,…[FTC] can't prohibit…collecting information." Mot. 16 n.12. They also concede that even FTC's 2008 Resolution did not claim authority to regulate data-security under a pure "unfairness" theory. *Cf.* Mot. 17 n.14.

FTC admits it pestered Congress to confer data-security authority, Opp. 14; *cf.* Mot. 15-16 nn.12-15, but argues that "FTC's requests for additional [data-security] authority showcase…FTC's unfairness authority," Opp. 13. This non-sequitur fails. Asking Congress for the authority to regulate data-security "showcases" only that FTC lacked this authority, for there would be no need to ask for power FTC already had.

FTC's recent statements claiming general Section 5 "unfairness" data-security authority cannot erase FTC's many prior statements disavowing Section 5 data-security jurisdiction or cloud the fact that Congress enacted many targeted data-security statutes against that backdrop.

FTC's reliance on *Smiley v. Citibank*, 517 U.S. 735 (1996), fails. First, here FTC's newfound Section 5 authority is a "[s]udden and unexplained change…." *Id.* at 742. Second, *Smiley* involved an agency regulation entitled to *Chevron* deference. *See id.* at 740-41. No deference is owed to FTC here, because it has not engaged in formal adjudication or rulemaking. *U.S. v. Mead Corp.*, 533 U.S. 218, 227 (2001).

2. Rejected Legislation Confirms FTC Lacks Authority.

FTC says "savings clauses" in four of *ten* or more bills Congress has rejected that would have given FTC general data-security authority supports its claimed authority. Opp. 14. This is bizarre.

First, all four cited bills were proposed in 2011, Opp. 14, *after* Congress had given FTC sector-specific data-security authority through GLBA, FRCA, and COPPA, Mot. 14 & n.10. Of course, these "[p]reservation clauses would be unnecessary if…FTC lacked existing authority," Opp. 14, under GLBA, FCRA, COPPA, and other targeted statutes. But the "savings clauses" are general, do not refer to Section 5, and protect FTC's data-security authority under these other statutes. *See* S. 1207, §6(d)(protecting "Commission's authority under any other provision of law"); H.R. 2577, §6(d)(same); H.R. 1841, §6(d)(same); H.R. 1707, §6(d)(same). None of these bills address, much less endorse, FTC's claimed Section 5 authority.[6] Indeed, H.R. 2577, §4(d)(1), would have *exempted* HIPAA-covered entities like LabMD from compliance.

Second, FTC ignores *six other* 2011 cybersecurity bills that included no language "preserving" FTC data-security authority. *See* S. 1151, S. 1408, S. 1434, S. 1535, S. 2105, H.R. 624.

D. *Massachusetts v. EPA* Supports LabMD's Arguments.

FTC's reliance on *Massachusetts v. EPA*, 549 U.S. 497 (2007), is misplaced. Unlike Section 5, the Clean Air Act unambiguously defined "air pollutant" to embrace "all airborne compounds of whatever stripe…." *Id.* at 528-29. Moreover, the Court noted two "critical" considerations absent from that case but present in *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000), and present here. *See Massachusetts*, 549 U.S. at 530-31. First, Section 5

[6] A single Senator's remark during a hearing has no weight, even if it did support FTC.

data-security jurisdiction for the *entire private economy* is not only "counterintuitive" but leads to "extreme measures," because it would require *substantive* data-security standards for the entire economy to be classified as "unfair" practices and eviscerate Congress's longstanding, deliberate policy of regulating data-security through narrow, targeted statutes. *Cf. id.*

Second, like *Brown & Williamson*, there is "an unbroken series of congressional enactments that ma[k]e sense only if adopted 'against the backdrop of…[FTC's] consistent and repeated statements that it lacked authority'" to regulate data-security. *Cf. id.* For FTC to prevail, Congress's many specific, narrow delegations of data-security regulatory authority enacted against the backdrop of FTC's repeated disavowal of general regulatory authority must be deemed superfluous nullities.[7] Furthermore, unlike *Massachusetts*, many of these statutes, including HIPAA/HITECH, directly conflict with FTC's claimed authority.

E. *ABA v. FTC* Illustrates Why Dismissal Is Required.

FTC dismisses *ABA v. FTC*, 430 F.3d 457 (D.C. Cir. 2005), claiming "there is no debate about the meaning of the term 'unfairness.'" Opp. 16 (citing 15 U.S.C. §45(n)). Given that the one court that actually considered FTC's claimed Section 5 authority to regulate patient-information data-security said "there is significant merit" to LabMD's argument against FTC's power-grab, *see* Mot. 1, and 15 U.S.C. §45(n) does not define "unfairness" but rather cabins FTC's authority,[8] that argument fails.

In truth, FTC concedes that nothing in Section 5 explicitly authorizes it to regulate patient-information data-security practices. Instead, as in *ABA*, FTC is simply grabbing power to "fill in" what it perceives as a regulatory gap. But Congress has already filled that "gap" through

[7] *See* Mot. 11-16 & nn.10-11 (listing and discussing specific statutes).

[8] Statutory language always trumps section titles. *R.R. Trainmen v. Balt.&Ohio R.R.*, 331 U.S. 519, 529 (1947).

HIPAA/HITECH, and FTC cannot second-guess Congress. FTC's assault on LabMD is contrary to the administrative structure Congress has constructed for patient-information data-security and entirely illegitimate. *See ABA*, 430 F.3d at 469-71.

Furthermore, FTC concedes Congress has generally left patient-information data-security to the states, and where Congress has found federal regulation of patient-information data-security practices appropriate, it has explicitly said so. *Cf.* Mot. 21; 42 U.S.C. §1320d-2(d)(1). Because Section 5 does not clearly authorize FTC's conduct here, its brazen power-grab must be denied. *See ABA*, 430 F.3d at 472.

II. FTC'S LACK OF STANDARDS VIOLATES DUE PROCESS.

A. FTC's Admitted Lack of Standards.

FTC admits LabMD has not violated any data-security statutes, rules, or regulations and concedes LabMD has not engaged in a "deceptive" trade practice. *Cf.* Mot. 6,8. It admits LabMD's data-security practices are regulated under HIPAA/HITECH and that HHS exclusively implements and enforces these statutes as applied to LabMD. *Cf.* Mot. 4,13. FTC's sole claim against LabMD is unspecified "unfair" acts or practices. *Cf.* Mot. 7-8.

FTC also admits that Section 5 statutorily bars FTC from enforcing consent orders against non-parties and that its consent orders do not establish illegal conduct and only bind the parties thereto. *Cf.* Mot. 23,26. It has not alleged LabMD had actual notice of the business guides, consumer alerts, links to Sans Institute/NIST publications, and other Internet postings. *Cf.* Mot. 24-28 & nn.19-21. It admits that none of these materials were published in the Federal Register and that *none* of their alleged sources of data-security standards create *any* legally binding duties and obligations. *Cf.* Mot. 7-8. Instead, FTC says Section 5 alone provides

constitutionally and statutorily adequate *ex ante* notice of what data-security practices are forbidden or required. Opp. 16-17.

B. Section 5 Does Not Establish Proper Standards.

FTC does not acknowledge, much less address, the authorities cited by LabMD holding that FTC was required to provide fair notice of prohibited or required conduct. FTC has never alleged that LabMD's patient-information data-security practices did not meet objective medical-industry standards in effect and applicable to businesses of its size and nature at the time of the alleged violation. *Cf. S&H Riggers & Erectors v. OSHRC*, 659 F.2d 1273, 1280-83 (5th Cir. 1981)(reasonable-person standard divorced from industry standards or regulations violates due process). Instead, FTC *admits* that LabMD, a HIPAA-covered entity, always complied with HIPAA/HITECH regulations. *Cf.* Mot. 4,8,13.

No case has ever held, and no plausible argument can be made, that Section 5 provides constitutionally-adequate data-security fair notice. *See* Stegmaier & Bartnick, *Physics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 706 (2013)("[S]tatutory language does not provide notice of required data-security safeguards."). Section 5's broad "unfairness" prohibition, which does not even refer to "data security," let alone prescribe or proscribe data-security practices, is far more offensive than the statutes at issue in cases like *Connally v. General Constr. Co.*, 269 U.S. 385 (1926)(cited by LabMD but ignored by FTC) finding fair-notice due-process violations. And even if data-security "reasonableness" standards could provide regulated entities with constitutionally-adequate notice if codified in a regulation or statute, FTC says it has not done so and will not do so.

To claim fair notice, FTC again distorts the law. It cites *U.S. v. Merrill*, 513 F.3d 1293, 1306 (11th Cir. 2008), but this is not a fair-notice case. The cherry-picked portion of *Merrill* it cites discusses *a jury instruction*, not statutory fair notice. Opp. 18. Unlike Section 5, the *Merrill* statute (Controlled Substance Act, 21 U.S.C. §841) is quite detailed and hence provides fair notice.

FTC claims OSHA's General Duty Clause is the best analogy to their standardless *ex post* data-security regime. Opp. 19 n.12. It is a poor fit. Cases interpreting OSHA's General Duty Clause prove LabMD's point and confirm why FTC's actions violate due process, particularly because FTC admits LabMD has always complied with HIPAA/HITECH's specific data-security requirements.

The General Duty Clause is a regulatory tool of last resort—a stop-gap—which "was not meant…[as] 'a general substitute for reliance on standards'" and only applies to "'special circumstances for which no standard has yet been adopted.'" *Ramsey Winch v. Henry*, 555 F.3d 1199, 1205 (10th Cir. 2009). It only controls where there are no other standards, because "standards preempt the [G]eneral [D]uty [C]lause…." *In re Samsonite Corp.*, 756 F. Supp. 498, 500 (D.Colo. 1991). FTC claims that even though LabMD has always complied with HIPAA/HITECH *data-security standards*, it remains liable under Section 5 for compliance with FTC's unstated data-security standards. This is the antithesis of how the General Duty Clause works.[9] *See Teal v. E. I. du Pont*, 728 F.2d 799, 804 (6th Cir. 1984)(Congress "enacted…general duty clause to cover serious hazards…not otherwise covered by specific regulations.").

[9] *See* OSHA's Field Operations Manual, CPL02-00-148, pp.4-14-4-30 (2009)(detailed elements of General-Duty-Clause violation and strict limits). Unlike Section 5, there are 30-plus years of concrete agency guidelines specifying General-Duty-Clause-imposed obligations. *E.g.*, *ConAgra, Inc.*, 1983-84 O.S.H. Dec. (CCH) ¶26,420, 33,523 (1983)(formal agency interpretation).

The "objective" industry-specific reasonableness standard at issue in *Voegle v. OSHA*, 625 F.2d 1075 (3d Cir. 1980), is fundamentally different from what FTC is doing here. *Voegle* involved a fair-notice challenge to a construction-industry-specific *regulation* (not the General Duty Clause), *see id.* at 1077, far more specific than Section 5's text. Furthermore, *numerous* agency enforcement actions applying occupational-safety regulations far more specific than Section 5 have been dismissed on fair-notice grounds. *E.g.*, *Fabi Const. Co. v. SOL*, 508 F.3d 1077, 1088 (D.C. Cir. 2007); *Gates & Fox v. OSHRC*, 790 F.2d 154,156-57 (D.C. Cir. 1986).

FTC enforcement actions are fundamentally different from garden-variety tort suits, and common-law negligence cases do not displace the APA's and Fifth Amendment's due-process fair-notice requirements. *See Satellite Broadcasting v. FCC*, 824 F.2d 1, 3 (D.C. Cir. 1987). Also, given FTC admits LabMD has not engaged in "deception," *cf.* Mot. 4, their reliance on dicta from *In re Zappos.com*, No. 12-00325, 2013 U.S. Dist. LEXIS 128155 (D.Nev. 2013), is badly misplaced, for they omit mention of the court's decision to treat the data-security claims as "negligent misrepresentation claims" based on false website statements,[10] *id.* at *15-16.

FTC v. National Urological Group (NUG), 645 F. Supp. 2d 1167 (N.D.Ga. 2008), also deals with "deceptive" advertising allegations not at issue here. FTC itself has explained why "deception" actions do not raise the same fair-notice concerns as "unfairness" actions: "[U]nfairness is the set of general principles of which deception is a particularly well-established and streamlined subset." *Int'l Harvester*, 1984 FTC LEXIS at *246. Further, the *NUG* court found it critical that, unlike here, FTC had at least expressly defined "competent and reliable scientific evidence" (this definition is omitted from FTC's block-quote) and articulated a definite

[10] *Loschiavo v. City of Dearborn* (overruled) is also not a fair-notice case; inapposite dicta FTC cites refers to the test for whether a private-right-of-action-against-the-government exists under Section 1983. *See* 33 F.3d 548, 551 (6th Cir. 1994).

standard. *See* 645 F.Supp.2d at 1186. That standard is exponentially more detailed than FTC's proposed "reasonableness" standard here.

Unlike FTC's nebulous, standardless concept of data-security "unfairness," "deception" has a well-established, clear meaning in Section 5 and elsewhere in the law and does not raise the same fair-notice concerns. *E.g.*, FTC Policy Statement on Deception, appended to *Cliffdale Assoc., Inc.*, 103 F.T.C. 110, 174 (1984)(*detailed* explication of deception elements). Thus, "deception" cases cited by FTC do not support its fair-notice argument.

Tellingly, FTC's discussion of the "reasonableness" analysis they believe Section 5 requires contains no citations whatsoever and appears to be cut from whole cloth—the only citation on the page is *In re Zappos.com*, addressed above. Opp. 21.

FTC dismissively argues that "ascertainable certainty does not require agencies to provide…guidance at the level of detail…[LabMD] seems to think appropriate." Opp. 20. They brazenly admit that neither the Complaint nor the notice order prescribe *any* specific data-security practices LabMD *should* (let alone must) implement going forward. *Cf.* Mot. 8. Elsewhere, FTC has boldly stated that the argument that a regulated entity "did not know which standard it was supposed to follow…misses the point." Mot. 27 n.21. They blithely explain that they "do[] not endorse any [industry] standards"—"[they] don't say…how you should set up your router…[they] don't say you should have…white…and black lists for IP addresses"—because "[they] are not tech support." Hearing Transcript, *FTC v. Wyndham*, 53:2-10 (Nov. 7, 2012).

The cases they cite—like the cases LabMD cites to which they do not bother to respond, *see* Mot. 22-28 & nn.19-21—make clear that this violates due process. For example, *U.S. v. Lachman*, 387 F.3d 42 (1st Cir. 2004), which, unlike here, involved a detailed technical

regulation and interpreted the phrase "specially designed," *id.* at 50-53, notes that the line of D.C. Circuit cases LabMD cites (and FTC ignores) invalidate agency *ex post* enforcement actions where, as here, the statute "is so ambiguous that a regulated party cannot be expected to arrive at the correct interpretation using standard [interpretive] tools…, must therefore look to the agency for guidance, and the agency failed to articulate its interpretation before imposing a penalty," *id.* at 57. Indeed, even FTC's patchwork-quilt of consent orders is inconsistent. *See* Stegmaier & Bartnick, *supra*, at 700 ("FTC has not explained why data-security practices in one [fact-specific consent-order] case may violate Section 5 while those same practices may not violate Section 5 in another case…apparently expect[ing] entities to piece together…complaints and consent orders in thirty-six cases, without any authoritative commentary, to arrive at…[FTC's] interpretation of adequate data-security practices….").

Finally, again without responding to LabMD's arguments and thereby conceding the points, *cf.* Mot. 25-26 & n.19, FTC—incredibly—suggests that NIST and HIPAA publications supply standards LabMD should have followed. Opp. 22 n.15. The NIST Handbook they cite is from 1995, does "not…specify requirements," and only "provides a broad overview of computer security." NIST, Special Publication, 800-12, §1.1 (1995). Section 1.1 of NIST Special Publication 800-30 states: "The guidelines herein are not mandatory and binding standards." With respect to HIPAA Guidance they cite, even if LabMD was required to follow it, FTC has admitted that LabMD *has always complied with all data-security obligations under HIPAA/HITECH.*

C. FTC Cannot Announce New Rules Through Adjudication Punishing Past Conduct.

The fact that, subject to fair notice, FTC may fill in Section 5's interstices through adjudication does not allow FTC to deliberately evade its constitutional and statutory fair-notice

obligations. FTC cannot regulate through intimidation by bullying companies into signing consent decrees. Yet FTC brags about the myriad consent decrees secured from 2005 to present, Opp. 12-13 n.9, and says they are "not obligated to engage in a rulemaking…," Opp. 23. *SEC v. Chenery*, 332 U.S. 194 (1947), where, unlike here, the agency "had not previously been confronted with the problem," *id.* at 203, explains that "[t]he function of filling in…[statutory] interstices…should be performed, as much as possible, through…quasi-legislative promulgation of rules to be applied in the future," *id.* at 202. *Chenery* is not a fair-notice case; unlike here, SEC did not seek liability for past conduct, *see id.* at 203-04. *PBW Stock Exch. v. SEC*, 485 F.2d 718 (3d Cir. 1973), also not a fair-notice case, involved *a challenged regulation*, not adjudication, *id.* at 721; dicta FTC cites is inapposite.

In *Beazer v. EPA*, 963 F.2d 603 (3d Cir. 1992), EPA had actually promulgated regulations through normal notice-and-comment rulemaking and the statute and regulations prescribed detailed requirements, *see id.* at 604-05. In that context, the court found adjudication permissible. *Cf. id.* at 609 (APA "expressly prohibit[s]…agency from retroactively imposing…interpretive rule upon…regulated party."). Unlike *Beazer*, here FTC brazenly admits that they do not have legislative or even interpretive rules explaining what data-security practices they believe Section 5 forbids or requires. *Cf. id.* at 606.

NLRB v. Bell Aerospace, 416 U.S. 267 (1974), is not a fair-notice due-process case and thus inapposite. Rather, the issue was Bell Aerospace's *future* collective-bargaining obligations. *See id.* at 269. Even in that very different context, the Court recognized situations where NLRB reliance on adjudication would be unlawful, noting that "this is not a case in which some new liability is sought to be imposed…for past actions" and that "fines or damages" were not involved. *Id.* at 294-95. Due-process-based fair-notice requirements are heightened where, as

here, the agency alleges violation of law based on *past* conduct. *See PMD Produce Brokerage v. USDA*, 234 F.3d 48, 51-52 (D.C. Cir. 2000).

III. FTC'S FAILURE TO STATE PLAUSIBLE SECTION 5 VIOLATION.

FTC concedes it lacks even *one* complaining witness who has suffered *any* injuries because of LabMD's alleged patient-information data-security failures. FTC admits LabMD complied with HIPAA/HITECH—the only applicable patient-information data-security requirements. FTC does not allege what the objective medical-industry-standard data-security practices are or were or that LabMD's data-security practices fell short of meeting them. As explained above, the *Iqbal/Twombly* standard applies here. The Complaint fails to meet that standard and must be dismissed.

IV. STAY NECESSARY TO STOP DISCOVERY ABUSE.

FTC does not deny that its discovery tactics are barred in federal courts and does not substantively respond to LabMD's arguments or deny LabMD's assertions. At minimum, the Commission should stay the proceedings.

CONCLUSION

For the foregoing reasons, LabMD respectfully requests that the Commission GRANT its Motion in full.

PUBLIC

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
Senior Vice President for Litigation and
Counsel to Cause of Action

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: December 2, 2013

CERTIFICATE OF SERVICE

I hereby certify that on December 2, 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.
John Krebs, 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: December 2, 2013 By: /s/ Michael D. Pepson

EXHIBIT 13

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**
	)	

ORDER DENYING RESPONDENT LABMD'S MOTIONS FOR STAY

In two separate motions, Respondent LabMD, Inc. ("LabMD") has requested that the Commission stay the ongoing proceeding before the Administrative Law Judge in this case. First, as part of its Motion to Dismiss with Prejudice and to Stay Administrative Proceedings, filed on November 12, 2013 ("Motion to Dismiss"), LabMD requested a stay pending our resolution of the merits of that motion. *See* Motion to Dismiss at 29-30. Second, on November 26, 2013, LabMD filed a Motion to Stay Proceedings Pending Review in the U.S. Court of Appeals for the Eleventh Circuit and the U.S. District Court for the District of Columbia ("Motion for Stay Pending Judicial Review").

For the reasons set forth below, we deny both the stay request incorporated into LabMD's Motion to Dismiss and LabMD's Motion for Stay Pending Judicial Review. In this Order, we do not address the merits of LabMD's Motion to Dismiss.

BACKGROUND

This case concerns allegations that LabMD – a provider of clinical laboratory testing services – failed to implement reasonable and appropriate measures to prevent unauthorized access to consumers' personal data stored on its computer systems. The Complaint initiating this case, issued on August 28, 2013 ("Complaint"), alleges that, as a result of LabMD's inadequate data security practices, identity thieves were able to obtain access to highly sensitive information – including patients' names combined with their dates of birth, social security numbers ("SSNs"), and information about their bank accounts, insurance coverage, or lab test results. *See* Complaint at 2-5 (¶¶ 6-21). The Complaint alleges that LabMD's conduct constituted an "unfair act or practice," in violation of Section 5(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a). *See* Complaint at 5 (¶¶ 22-23).

LabMD filed its Answer to the Complaint on September 17, 2013 ("Answer"), and as noted above, filed a Motion to Dismiss on November 12, 2013. Complaint Counsel filed a

Response in Opposition to the Motion to Dismiss ("CC Opp. to MTD") on November 22, 2013; and LabMD filed a Reply on December 2, 2013. The deadline for a Commission order resolving the merits of LabMD's Motion to Dismiss is January 16, 2014. *See* 16 C.F.R. §§ 3.22(a), 4.3(a). Factual discovery in this proceeding is scheduled to close on March 5, 2014, and the evidentiary hearing before the Administrative Law Judge is scheduled to begin on May 20, 2014. *See* Administrative Law Judge's Revised Scheduling Order (issued Oct. 22, 2013).

On November 14, 2013, LabMD filed a Verified Complaint for Declaratory Relief against the Commission in the U.S. District Court for the District of Columbia (docketed as Case No. 1:13-cv-01787-CKK) ("District Court Complaint"). On November 18, 2013, LabMD filed a "Petition for Review of Unlawful Federal Trade Commission Attempt to Regulate Patient-Information" in the U.S. Court of Appeals for the Eleventh Circuit (docketed as Case No. 13-15267) ("11th Circuit Petition"). On November 26, 2013, LabMD filed its Motion for Stay Pending Judicial Review in this proceeding. Complaint Counsel filed an Opposition to the latter motion on December 5, 2013. ("CC Opp. to MSPJR").

ANALYSIS

I. Request for Stay Pending a Decision on the Merits of LabMD's Motion to Dismiss

Our rules provide that, as a general matter, a motion to dismiss filed prior to evidentiary hearings is to be referred directly to the Commission for decision, 16 C.F.R. § 3.22(a), and the fact that such a motion is pending "shall not stay proceedings before the Administrative Law Judge unless the Commission so orders." *Id*. § 3.22(b). When we most recently revised this rule, we stated that that the "purpose of . . . paragraph (b) is to ensure that discovery and other prehearing proceedings continue while the Commission deliberates over the dispositive motions, . . . [so as] to expedite the proceedings." FTC, *Rules of Practice*, Interim Final Rules with Request for Comment, 74 Fed. Reg. 1804, 1809, 1810 (Jan. 13, 2009).

In deciding whether to grant LabMD's request for a stay of the proceeding pending our resolution of its Motion to Dismiss, we exercise our discretion to oversee this adjudication, comparable to the broad discretion of a court "to stay proceedings[,] . . . incidental to the power inherent in every court to control the disposition of the [cases] on its docket with economy of time and effort for itself, for counsel, and for litigants. How this can best be done calls for an exercise of judgment." *Landis v. North Am. Co.*, 299 U.S. 248, 254 (1936). We conclude that there is no good cause for the stay LabMD requests.

LabMD contends that a stay pending resolution of the merits of its Motion to Dismiss is justified, in part, because Complaint Counsel has sought "extensive and abusive discovery" that would impose "ruinous litigation costs" on the company. Motion to Dismiss at 29, 30. Complaint Counsel responds that this argument is no more than a "rehash" of arguments over third-party discovery that are already pending before the Administrative Law Judge. CC Opp. to MTD at 26. Significantly, the Administrative Law Judge recently issued an order resolving pending discovery disputes. *See* Administrative Law Judge's Order on Respondent's Motion for a Protective Order at 7-8 (issued Nov. 22, 2013). By precluding discovery on conduct prior to 2005 and discovery of materials relating to a book by LabMD's CEO, this Order may ameliorate

LabMD's burdens and costs to some extent. If further disputes between LabMD and Complaint Counsel emerge during the course of the discovery process, the Administrative Law Judge is well equipped to address them in the first instance.

LabMD further argues that a stay pending resolution of the Motion to Dismiss would be proper because "[f]orcing LabMD to litigate a case that the Commission does not even have jurisdiction to bring is inherently unjust and violates its due process rights." Motion to Dismiss at 30. Without expressing any view on the merits of the Motion to Dismiss, we conclude that the fact that LabMD has challenged the Commission's authority to bring this case does not justify a stay. As discussed above, when we adopted the current version of Section 3.22 of our Rules of Practice, we anticipated that parties might file dispositive pre-hearing motions, but concluded that the public interest in expediting our adjudicatory process supports allowing the proceedings before the Administrative Law Judge to continue notwithstanding the pendency of such motions. Thus, in past adjudications, we have declined to grant motions for stay of pretrial proceedings pending resolution of motions to dismiss.[1] Consistently, reviewing courts have held that litigants must participate fully in the Commission's adjudications even where they "have challenged the very authority of the agency to conduct proceedings against them." *Ticor Title Ins. Co. v. FTC*, 814 F.2d 731, 739 (D.C. Cir. 1987) (opinion of Edwards, J.). The Supreme Court has clearly ruled that the "expense and disruption [incurred by the respondent in] defending itself in protracted adjudicatory proceedings" before the Commission do not justify halting those proceedings prior to their conclusion, even where, as here, the respondent "alleged unlawfulness in the issuance of the complaint." *FTC v. Standard Oil Co. of Cal.*, 449 U.S. 232, 244 (1980).

II. Motion for Stay Pending Judicial Review

Under our rules, "[t]he pendency of a collateral federal court action that relates to the administrative adjudication shall not stay the proceeding unless a court of competent jurisdiction, or the Commission for good cause, so directs." 16 C.F.R. § 3.41(f). The stay of administrative proceedings pending judicial review sought by LabMD, like stays of trial court proceedings pending appellate review in federal court, would be "an intrusion into the ordinary processes of administration and judicial review." *Nken v. Holder*, 556 U.S. 418, 427 (2009) (quoting *Virginia Petroleum Jobbers Ass'n v. FPC*, 259 F.2d 921, 925 (D.C. Cir. 1958)). Thus, a party requesting a stay in an administrative adjudication – as in federal court – bears the burden of demonstrating that the applicable criteria are fully satisfied.[2] "The first two factors of the traditional standard" – likelihood of success and irreparable injury – "are the most critical." *Id.* at 434.

---

[1] *See, e.g., N.C. State Bd. of Dental Exam'rs*, 150 F.T.C. 851 (2010). The U.S. District Court denied the same respondent's motion to halt the same pending proceeding. *See N.C. State Bd. of Dental Exam'rs v. FTC*, 768 F. Supp. 2d 818, 820 n.1 (E.D.N.C. 2011).

[2] Our procedural decisions in administrative adjudications are governed by the FTC Act and our own Rules of Practice, rather than the rules and standards that govern federal courts. The same factors, however, apply to motions for stay pending appeal in both types of fora. *Compare* 16 C.F.R. § 3.56(c) (factors governing stay motions under 15 U.S.C. § 45(g)(2) and 16 C.F.R. § 3.56(a)), *with Hilton v. Braunskill*, 481 U.S. 770, 776 (1987) (factors under Fed. R. Civ. P. 62(c) and Fed. R. App. P. 8(a)). These factors are: "[1] the likelihood of the applicant's success on appeal; [2] whether the applicant will suffer irreparable harm if a stay is not granted; [3] the degree of injury to other parties if a stay is

Applying this analytical framework, we conclude LabMD has failed to satisfy its burden of showing "good cause" to grant its Motion for Stay Pending Judicial Review.[3]

A. Likelihood of Success on the Merits

A party seeking a stay must "make a strong showing that [it] is likely to succeed on the merits . . . . [M]ore than a mere 'possibility' of relief is required." *Nken*, 556 U.S. at 434. LabMD has not shown that it is likely to prevail on the merits before the District Court or the Eleventh Circuit. We reach this conclusion without addressing the substantive merits of LabMD's District Court Complaint or 11th Circuit Petition – both of which present issues that substantially overlap the substantive issues LabMD raised in its Motion to Dismiss pending before us, which we are not considering or addressing in this Order. Nonetheless, we conclude that neither the District Court nor the Eleventh Circuit is likely to grant LabMD's request for declaratory or injunctive relief to halt this adjudication.

First, neither the District Court nor the Court of Appeals has jurisdiction to entertain LabMD's premature challenge to this adjudicatory proceeding. The FTC Act sets forth a detailed judicial review scheme that makes clear that a respondent in a Section 5 adjudication may obtain judicial review *only* if it (1) identifies "an order of the Commission" requiring it "to cease and desist from using any method of competition or act or practice;" (2) files "a written petition praying that the order of the Commission be set aside" with one of a specified set of U.S. Courts of Appeals; and (3) does so "within sixty days of the service of such order." 15 U.S.C. § 45(c). The Act also makes clear that this judicial review process implicates the courts' jurisdiction. *See id.* (filing of such petition triggers the court's "jurisdiction"); *id.*, § 45(d) ("[T]he jurisdiction of the [C]ourt of [A]ppeals of the United States to affirm, enforce, modify, or set aside orders of the Commission shall be exclusive."). Statutory requirements specifying which courts may review which types of agency decisions – such as provisions limiting judicial review to agency rulings that "are 'final' and 'made after a hearing'" – are deemed "central to the requisite grant of subject-matter jurisdiction." *Weinberger v. Salfi*, 422 U.S. 749, 764 (1975). Where, as here, it is "fairly discernible" from the text and overall structure of a statute that Congress intended that appeals of agency actions "proceed exclusively through the statutory review scheme," then that statute "precludes . . . courts from exercising jurisdiction over [a] pre-enforcement challenge" outside the prescribed procedures, and does not allow parties to "evade the statutory-review process by enjoining the [agency] from commencing enforcement proceedings, as petitioner sought to do here." *Thunder Basin Coal Co. v. Reich*, 510 U.S. 200, 216 (1994); *accord Elgin v. Dept. of Treasury*, 132 S. Ct. 2126, 2132-33 (2012).

---

granted; and [4] whether the stay is in the public interest." 16 C.F.R. § 3.56(c). *See also N.C. State Bd. of Dental Exam'rs*, 151 F.T.C. 640 (2011) (denying respondent's motion for stay pending district court review).

[3] LabMD's request that the Commission rule on this motion by December 5, 2013 – a day before the due date for Complaint Counsel's response – is now moot. *See* Motion for Stay Pending Judicial Review at 8; 16 C.F.R. § 3.22(d).

Both LabMD's District Court Complaint and its 11th Circuit Petition fail this test. "The District Court is without jurisdiction to enjoin hearings because the power 'to prevent any person from engaging in any unfair practice affecting commerce' has been vested by Congress in the [agency] and in the Circuit Court of Appeals . . . ." *Myers v. Bethlehem Shipbuilding Co.*, 303 U.S. 41, 48 (1938).[4] And the Court of Appeals is authorized by the FTC Act to review only an "order of the Commission to cease and desist from using any method of competition or act or practice." 15 U.S.C. § 45(c). *See Texaco, Inc. v. FTC*, 301 F.2d 662, 662 (5th Cir. 1962) (per curiam) ("The jurisdiction of this Court to review an order of the Federal Trade Commission is found in 15 U.S.C. § 45(c). Such jurisdiction arises only from a cease and desist order entered by the Commission."). The Commission has issued no cease and desist order in this proceeding.

LabMD's attempt to short-circuit this adjudicatory proceeding by going straight to court is "at war with the long-settled rule of judicial administration that no one is entitled to judicial relief for a supposed or threatened injury until the prescribed administrative remedy has been exhausted[,] . . . . [even] in cases where, as here, the contention is made that the administrative body lacked power over the subject matter." *Bethlehem Shipbuilding Corp.*, 303 U.S. at 50-51. *See also Ewing v. Mytinger & Casselberry, Inc.*, 339 U.S. 594, 599 (1950) ("it has never been held that the hand of government must be stayed until the courts have an opportunity to determine whether the government is justified" in instituting such proceedings). The law is clear that a party may not halt a legitimate law enforcement proceeding that a federal agency is conducting against that party by seeking an injunction or declaratory order, provided that the party has a meaningful opportunity to obtain judicial review after the proceeding concludes and a final order is issued. *See, e.g.*, *FTC v. Claire Furnace Co.*, 274 U.S. 160, 174 (1927) (where respondents have a "full opportunity to contest the legality of any . . . proceeding against them[,] . . . they [could] not . . . ask relief by injunction"); *cf. Thunder Basin Coal Co. v. Reich*, 510 U.S. at 212-13 (distinguishing *Leedom v. Kyne*, 358 U.S. 184 (1958) and its progeny).

Moreover, LabMD has no probability of success on the merits before either the District Court or the Eleventh Circuit because there is no "final agency action" in this proceeding. The Commission has merely averred "reason to believe" that violations have occurred and found "good cause" to issue a Complaint. "Serving only to initiate the proceedings, the issuance of the complaint has no . . . . legal or practical effect, except to impose upon [the respondent] the burden of responding to the charges made against it." *Standard Oil Co.*, 449 U.S. at 242. The Eleventh Circuit has found that "the 'final agency action' requirement implicates federal subject matter jurisdiction," *Nat'l Parks Conservation Ass'n v. Norton*, 324 F.3d 1229, 1240 (11th Cir. 2003), while the D.C. Circuit treats the absence of final agency action as a failure to state a claim upon which relief can be granted. *See, e.g.*, *Reliable Automatic Sprinkler Co. v. CPSC*, 324 F.3d 726, 731-32 (D.C. Cir. 2003). Either way, LabMD loses.

LabMD contends the Commission has already made up its mind, and therefore, further participation in this proceeding would be futile. *See, e.g.*, District Court Complaint at 25-26

[4] Although *Myers v. Bethlehem Shipbuilding Co.* concerned the National Labor Relations Act, the Court quoted and relied upon the legislative history of the FTC Act, which revealed Congress' unequivocal intent that this mode of review is exclusive. *See* 303 U.S. at 48 n.5.

(¶¶ 132-37). LabMD is wrong. "Although [respondent] claims that it is highly unlikely that the agency will change its position and that resort to the agency's adjudicatory proceeding would be futile, nothing in the record indicates that the outcome of a hearing, where [respondent] will have the opportunity to present its arguments to the agency, is preordained." *Reliable Automatic Sprinkler Co.*, 324 F.3d at 733. Even assuming, *arguendo*, that the Commission has expressed views in the past about some of the legal and policy issues in this case, that would "not necessarily mean that the minds of its members [are] irrevocably closed on the subject of respondents' . . . practices[,]" nor that they are "prejudiced and biased" against LabMD, so that it "could not receive a fair hearing from the Commission." *FTC v. Cement Inst.*, 333 U.S. 683, 700 (1948).[5] The Commission's ultimate ruling in this case "is contingent on a number of factors" – including an assessment of whether the facts alleged in the Complaint actually occurred, and whether those facts are sufficient to sustain a finding that LabMD committed unfair acts and practices. "Under these circumstances, where [a court] can have no idea whether or when [a sanction] will be ordered, the issue is not fit for adjudication." *Texas v. United States*, 523 U.S. 296, 300 (1998) (quoting *Toilet Goods Assn., Inc. v. Gardner*, 387 U.S. 158, 163 (1967).

B. Irreparable Harm

A party seeking a stay must show that it "will be irreparably injured absent a stay; simply showing some 'possibility of irreparable injury' fails to satisfy the second factor." *Nken*, 556 U.S. at 434-35. LabMD asserts that, absent a stay, the pendency of this proceeding "damages LabMD's business reputation, causing it to lose customer goodwill and market share," "threaten[s] the very existence of [its] business," and "eviscerates LabMD's due process rights." Motion for Stay Pending Judicial Review at 4-5. To be sure, "[t]he harm to property and business can . . . be incalculable by the mere institution of proceedings . . . . Yet it is not a requirement of due process that that there be judicial inquiry before discretion can be exercised" to commence an adjudication. *Mytinger & Casselberry Inc.*, 339 U.S. at 599. Indeed, "every respondent to a Commission complaint" – and every litigation defendant – "could make the [same] claim[.]" *Standard Oil Co.*, 449 U.S. at 242-43. "Irreparable harm cannot be established by a mere reliance on the burden of submitting to agency hearings. This is a risk of litigation that is inherent in society, and not the type of injury to justify judicial intervention." *Sears, Roebuck & Co. v. NLRB*, 473 F.2d 91 (D.C. Cir. 1972). "[T]he expense and annoyance of litigation is 'part of the social burden of living under government[,]' [and] . . . '[m]ere litigation expense, even substantial and unrecoupable cost, does not constitute irreparable injury." *Standard Oil Co.*, 449 U.S. at 244 (quoting *Petroleum Exploration, Inc. v. Pub. Serv. Comm'n*, 304 U.S. 209, 222 (1938), and *Renego. Bd. v. Bannercraft Clothing Co.*, 415 U.S. 1, 24 (1974)).

[5] *See also N.C. State Bd. of Dental Exam'rs*, Opinion Denying Respondent's Motion to Disqualify the Commission, 151 F.T.C. 644, 648-54 (2011) (citing, *inter alia*, *Cement Institute*, *Cinderella Career & Finishing Schools, Inc. v. FTC*, 425 F.2d 583 (D.C. Cir. 1970), and *Am. Med. Ass'n v. FTC*, 638 F.2d 443 (2d Cir. 1980)).

C. Effect on Other Parties and Public Interest

Finally, LabMD fails to satisfy the other relevant factors. Its contention that "[a] stay of this matter will injure no one at all," Motion for Stay Pending Judicial Review at 7, is ably countered by Complaint Counsel's argument that a stay could expose "consumers [to] the risk of identity theft, medical identity theft, and other harms." CC Opp. to MSPJR at 6. And needlessly delaying the pending adjudicatory proceeding could frustrate the public interest in expeditious resolution of adjudicatory matters. We cannot conclude that the stay sought by LabMD would be in the public interest.

Accordingly,

IT IS ORDERED THAT Respondent LabMD, Inc.'s request for a stay of administrative proceedings pending disposition of the merits of its Motion to Dismiss **IS DENIED;** and

IT IS FURTHER ORDERED THAT Respondent LabMD's Motion to Stay Proceedings Pending Review in the U.S. Court of Appeals for the Eleventh Circuit and the U.S. District Court for the District of Columbia **IS DENIED.**

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: December 13, 2013

EXHIBIT 14

UNITED STATES DISTRICT COURT.
FOR THE DISTRICT OF NEW JERSEY
Civil 13-1887 ES

FEDERAL TRADE COMMISSION,

Plaintiff, MOTIONS TO DISMISS

V.

WYNDHAM WORLDWIDE CORPORATION, ET AL,

DEFENDANTS.

- -

NEWARK, NEW JERSEY
NOVEMBER 7, 2012

B E F O R E: HONORABLE ESTHER SALAS,
UNITED STATES DISTRICT JUDGE

A P P E A R A N C E S:

KEVIN HYLAND MORIARTY, ESQ.
KRISTIN KRAUSE COHEN, ESQ.
JONATHAN ELI ZIMMERMAN, ESQ.
FOR THE FEDERAL TRADE COMMISSION.

GIBBONS
BY: JUSTIN T. QUINN, ESQ.
AND
KIRKLAND & ELLIS
BY: EUGENE ASSAF, ESQ.
AND: K. WINN ALLEN, ESQ.
For the Defendants.

Pursuant to Section 753 Title 28 United States Code, the following transcript is certified to be an accurate record as taken stenographically in the above-entitled proceedings.

S/LYNNE JOHNSON

- -

LYNNE JOHNSON, CSR, CM, CRR
OFFICIAL COURT REPORTER
UNITED STATES DISTRICT COURT
P.O. BOX 6822
LAWRENCEVILLE, NEW JERSEY 08648
CHJLAW@AOL.COM

THE COURT: Good morning to everyone. Please be seated.

We are on the record in the matter of Federal Trade Commission versus Wyndham Worldwide Corporation et al, civil 13-1887. Let me have appearances by counsel.

MR. MORIARTY: Kevin Moriarty on behalf of the Federal Trade Commission.

MR. ZIMMERMAN: Jonathan Zimmerman on behalf of the Federal Trade Commission.

MS. COHEN: Kristin Cohen for the FTC.

MR. QUINN: Justin Quinn for the defendants. Along with me at counsel table is Eugene Assaf, K. Winn Allen and Douglas Meal. Also with me are representatives from Wyndham, Marcus Banks and Korin Neff.

Mr. Assaf will be arguing the authority question. Mr. Allen will be answering any questions with respect to the common enterprise and if your Honor has any questions on the motion to stay, I will be addressing those.

THE COURT: Perfect. Be seated.

Let me tell you the order we are going to go today. We are going to start with whether Section 5, unfair authority extends to data security and if so,

MR. MORIARTY: We are pretty squarely within the fair notices category there. I think there are a lot of answers to that question, the principal one being that Wyndham in its privacy policy tells the consumers that they are going to take commercially reasonable steps to adequately protect their data. So you know, it is an objective standard, reasonableness, and for them to claim that it is now kind of a meaningless standard, it sort of rings hollow.

But as far as advisory opinions, there are not advisory opinions. But the way companies determine what is reasonable and what is not reasonable is the same way companies Act in any other legal context. The entire foundation of the common law negligence is requiring companies to Act reasonably under the circumstances. For example, in the context of data privacy they should evaluate the size and complexity of their network, evaluate the type of consumer data they are collecting and storing. They should evaluate industry standards. There are industry standards out there that are not associated with the FTC. There are experts out there that consult with companies routinely about the data security.

THE COURT: I am sorry to interrupt you,

counsel.

Does the FTC sort of endorse any particular industry standards that are out there? Are they published? How is that information disseminated in terms of what the industry standard should be?

MR. MORIARTY: Industry standards are well known. There are industry standards that specifically apply to the collection and transmission of credit card data. The FTC does not endorse any standards, particular standards. There is a Third Circuit case called Vogel which talked about whether a reasonableness standard should be pinned to industry standards. The Third Circuit said no, it should evaluate other reasonable things that companies in that position should look at.

The other thing I wanted to mention about FTC guidance is we have these books that we issue, guidance books. Also the adjudications are very valuable.

In this case in particular, I think it is that at page 19 of our brief, we identify a good number of the other, there is, at the time we wrote the brief, there were 19 unfairness cases. I think there is two more that are public. But we identified the particular types of things that companies should

be looking for in order to evaluate whether their data security is reasonable.

Now, we don't say here is how you should set up your router. We don't say you should have, you know, white lists and black lists for IP addresses. We are not tech support. We do say to them, companies, these are the types of things the FCC is looking at, you should make sure your house is in order on these things. The FTC provides guidance through these opinions, through these consent decrees.

THE COURT: Thank you. I will let you address any points you want to address after counsel argues with respect to whether the FTC has provided fair notice.

MR. MORIARTY: Thank you, your Honor.

THE COURT: Thank you. Mr. Assaf.

MR. ASSAF: May I have permission to make two reply points?

THE COURT: Sure.

MR. ASSAF: First of all, with respect to the FTC's point that Graham-Leach-Bliley, COPPA, that these were all cases in which Congress enacted them in order to avoid the FTC having to prove injury. That was kind of how they reconcile these cases. First of all, that is not in their brief. In fact, on page 12

section, your Honor, that Graham-Leach-Bliley, the Fair Credit Reporting Act, and COPPA, they have authority to publish rules. But under Section 57 (a) they also have the authority to prescribe rules and general statements of policy, and they have not done that for data security. There is no dispute about that.

This is where again it is not just Wyndham. I would suggest there is academic commentary saying the nature, format and content of the agency's data security related pronouncements raise equitable considerations that create serious due process concerns, what I call fair notice.

So what are the arguments?

Now, I understand, your Honor, I am going to get to the agency's arguments, and I understand that these are requests for admissions, but I think they actually filed them in this Court. And again, there is not any dispute here. The FTC has not published public information about what security software should be used by a company. Admitted.

And the FTC has not published any substantive rules or regulations pursuant to their statutory authority explaining what data security protections an individual or entity must employ to be in compliance.

unreasonable security practices. We are in court, I will make this argument. The FTC he will never ever worry about a motion to dismiss under their view. All they have to say is we alleged unreasonable security practices. Let's go forward with discovery. That is all they have to allege, no matter what the violation is.

So your Honor, I have no way, as a defendant, to know what I need to do to stay out of the FTC's aim, or more importantly what I can do in front of an Article III Judge to say, here re the regulations with ascertainable certainty, and my client abided by those regulations. Right now, I can't do either. And I think that is inconsistent with the Third Circuit law. Then we get to deception.

So I am happy to answer any questions, your Honor, but that is the outline of my argument. Again, I don't think there is going to be any dispute that there are rules or regulations, there are none out there.

Thank you, your Honor.

THE COURT: Okay. I will hear from counsel for the FTC.

Do you concede there are no rules and regulations that are currently available?

MR. MORIARTY: Regarding FTC Act liability, no, there aren't for data security. There are for GLB, which counsel pointed out. Graham-Leach-Bliley regulations were issued by the SEC, which goes back to the expertise.

I actually would like to touch on the guidelines from GLB for just a second. Those are the guidelines that if a company violates those guidelines they can be held liable under the FTC Act without injury.

The guidelines, if you look at them, require companies, I mean there are several, I think there are four different steps, but sort of the linchpin of the guidelines is that companies must take steps that are reasonably designed to protect consumer data. And this idea that through the GLB guidelines the FTC has created very elaborate technological regimes where companies can know precisely how to protect their data is inaccurate.

Just to step back for a second, I think the basic premise of Wyndham's fair notice argument is that they don't know how to comply with the reasonableness standard when it comes to protecting consumer information. The argument is problematic. First Wyndham states in its privacy policy it is going

time.

So the last point that I want to make is with these consent decrees, there are consent decrees and then there are also complaints. And the idea that they are not binding on this Court, we don't argue that they are binding on this Court. It is a red herring.

What we argued, the purpose of decrees is to provide parties with notice about the application of the FTC Act and about the types of things that the FTC evaluates when determining whether a company is engaged in reasonable practices with regards to consumer data.

THE COURT: So you say, counsel is arguing that they are not binding, and you never submitted that they are binding. But what you are saying, the real issue here is do these consent decrees provide notice to businesses as to what you need to be doing, and if you are not doing, there is danger.

And so you say that by -- counsel, I don't know whether it was in, it is probably in the reply brief, one of the things they say is all these consent decrees are very -- they are a case that deals directly with this particular company. And it is very difficult for us to say, well, based on those facts

are we in danger? And that they don't provide, you know, adequate warning or adequate notice as to what they need to be doing. And you would say what to that?

MR. MORIARTY: So the answer is that they do provide a lot of information, but we are not exclusively leaning on those adjudications, those consent decrees and complaints as the only source of fair notice. Nor would industry, I believe, accept it if the FTC stated we are the sole arbiter of what is reasonableness.

Reasonableness is an objective standard. It is not the FTC's reasonableness and Wyndham's reasonableness. Reasonableness is objective. There are a lot of sources companies can look to. There is no single answer. That is what happens all the time in the law.

So if a company is trying to figure out, if the grocery store is trying to avoid slip and fall accidents, the common law that they might look at won't be exactly their grocery store, you know, circumstances won't be the same, the type of threats to consumers might not be the same, but they can still make reasonable judgments based on previous cases and a variety of industry standards and just the general

Exhibit E

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

LABMD, INC.,	)	
	)	
Plaintiff,	)	
	)	Case 1:14-cv-00810-WSD
v.	)	
	)	
FEDERAL TRADE COMMISSION,	)	
	)	
Defendant	)	
_____	)	

DEFENDANT FTC'S CONSOLIDATED BRIEF IN SUPPORT OF ITS MOTION TO DISMISS AND IN OPPOSITION TO PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

INTRODUCTION 3

BACKGROUND 5

I. Legal framework 5

II. The administrative investigation and complaint 6

III. LabMD's multiple federal court challenges to the ongoing administrative proceedings 10

ARGUMENT 11

I. The complaint must be dismissed for lack of jurisdiction 11

A. This Court lacks jurisdiction to consider any of LabMD's claims because doing so would interfere with the ongoing FTC proceeding 12

1. This Court lacks jurisdiction over pre-enforcement challenges to an administrative adjudication 12

2. This Court cannot enjoin the ongoing administrative proceedings. 15

B. LabMD's claims are all patently unripe. 17

C. The Court lacks jurisdiction over plaintiff's APA claim, which does not challenge final agency action. 20

II. In the alternative, the complaint should be dismissed for failure to state a claim 25

A. Plaintiff fails to state a valid claim that the FTC lacks power to regulate data security 26

B. Plaintiff's other *ultra vires* claims also fail under 12(b)(6). 30

C. Plaintiff fails to make a valid "fair notice due process" claim 32

1. Plaintiff's claim does not implicate a liberty or property interest 32

2. Due process does not require the FTC to issue data security regulations before bringing an enforcement action against LabMD 33

3. The FTC is not employing an unconstitutionally vague standard. 35

D. Plaintiff does not make a valid "structural due process" claim 36

1. The FTC's structure and Rules of Practice do not violate due process 37

2. Plaintiff has no valid ex post facto claim 40

E. Plaintiff's First Amendment claims must be dismissed under Rule 12(b)(6). 41

III. LabMD's motion for a preliminary injunction must be denied. 44

CONCLUSION 47

TABLE OF AUTHORITIES

FEDERAL CASES

ACLU of Fla., Inc. v. Miami-Dade Cnty. Sch. Bd.,
557 F.3d 1177 (11th Cir. 2009) 47

All Care Nursing Serv., Inc. v. Bethesda Mem'l Hosp., Inc.,
887 F.2d 1535 (11th Cir. 1989) 47

Alliance for Natural Health U.S. v. Sebelius,
775 F. Supp. 2d 114 (D.D.C. 2011) 38

Am. Fin. Servs. Ass'n v. FTC,
767 F.2d 957 (D.C. Cir. 1985) 30, 36

Am. Gas Ass'n v. FERC,
912 F.2d 1496 (D.C. Cir. 1990) 35

Arnold v. CFTC,
987 F. Supp. 1463 (S.D. Fla. 1997) 47

Arthur Murray Studio of Wash., Inc. v. FTC,
458 F.2d 622 (5th Cir. 1972) 42

Ashcroft v. Iqbal,
556 U.S. 662 (2009) 25, 26, 34

Athlone Indus. Inc. v. Consumer Prod. Safety Comm'n,
707 F.2d 1485 (D.C. Cir. 1983) 23, 24

Atl. Refining Co. v. FTC,
381 U.S. 357 (1965) 30

Bd. of Regents of State Colleges v. Roth,
408 U.S. 564 (1972) 34, 35

Bell Atl. Corp. v. Twombly,
550 U.S. 544 (2007) 25, 26, 44

Blum v. Bankatlantic Fin. Corp.,
925 F.2d 1357 (11th Cir. 1991) 48
Branch v. Smith,
538 U.S. 254 (2003) 28
Butz v. Economou,
438 U.S. 478 (1978) 47
Cafeteria Workers v. McElroy,
367 U.S. 886 (1961) 39
Carpenter v. Com. of Penn.,
58 U.S. 456 (1854) 43
Chevron v. NRDC,
467 U.S. 837 (1984) 24
City of Arlington v. FCC,
133 S. Ct. 1863 (2013) 29
CSI Aviation Servs. v. US Dep't of Transportation,
637 F.3d 408 (D.C. Cir. 2011) 23
Digital Properties, Inc. v. City of Plantation,
121 F.3d 586 (11th Cir. 1997) 17
Direct Mktg. Concepts, Inc. v. FTC,
581 F. Supp. 2d 115 (D. Mass. 2008) 17
Dufrense v. Baer,
744 F.2d 1543 (11th Cir. 1984) 43
Elgin v. Dept. of Treasury,
132 S. Ct. 2126 (2012) 13
Ewing v. Mytinger & Casselberry, Inc.,
339 U.S. 594 (1950) 11, 15, 16, 48

Freeman United Coal Min. Co. v. Federal Mine Safety & Health Review Comm'n,
108 F.3d 358 (D.C. Cir. 1997) 38, 39

Frito-Lay, Inc. v. FTC,
380 F.2d 8 (5th Cir. 1967) 14, 28

FTC v. Accusearch, Inc.,
570 F.3d 1187 (10th Cir. 2009) 31

FTC v. Cement Inst.,
333 U.S. 683 (1948) 40

FTC v. Cinderella Career & Finishing Schs, Inc.,
404 F.2d 1308 (D.C. Cir. 1968) 40

FTC v. Colgate-Palmolive Co.,
380 U.S. 374 (1965) 36

FTC v. Neovi, Inc.,
604 F.3d 1150 (9th Cir. 2010) 31

FTC v. R.F. Keppel & Bro., Inc.,
291 U.S. 304 (1934) 30

FTC v. Sperry & Hutchinson Co.,
405 U.S. 233 (1972) 31

FTC v. Standard Oil,
449 U.S. 232 (1980) .....passim

Harris v. Mexican Specialty Foods, Inc.,
564 F.3d 1301 (11th Cir. 2009) 38

Holt Cargo Sys. v. Delaware River Port Auth.,
20 F. Supp. 2d 803 (E.D. Pa. 1998) *aff'd* 165 F.3d242 (3d Cir. 1999)..... 34

Houston v. Williams,
547 F.3d 1357 (11th Cir. 2008) 43

Intercontinental Indus., Inc. v. Am. Stock Exch.,
452 F.2d 935 (5th Cir. 1971) 40
J.E.M. Ag. Supply, Inc. v. Pioneer Hi-Bred Int'l, Inc.,
534 U.S. 124 (2001) 27
LabMD v. FTC,
No. 1:13-cv-1787 (Nov. 14, 2013 D.D.C.) 6, 10
Lauren v. DeFlaminis,
480 F.3d 259 (3d Cir. 2007) 45
Longshoremen v. Boyd,
347 U.S. 222 (1954) 19
McElmurray v. Consol. Gov't Augusta-Richmond Cnty,
501 F.3d 1244 (11th Cir. 2007) 11
Morrissey v. Brewer,
408 U.S. 471 (1972) 39
Moton v. Cowart,
631 F.3d 1337 (11th Cir. 2011) 44
Myers v. Bethlehem Shipbuilding Corp.,
303 U.S. 41 (1938) 15
N.C. Bd. Dental Examiners v. FTC,
768 F. Supp. 2d 818 (E.D.N.C. 2011) 16
Nat'l Parks Conservation Ass'n v. Norton,
324 F.3d 1229 (11th Cir. 2003) 20
NW Airlines v. Transp. Workers Union of Am.,
451 U.S. 77 (1981) 36
Ohio Forestry Ass'n v. Sierra Club,
523 U.S. 726 (1998) 18, 25

Olitsky v. O'Malley,
597 F.2d 295 (1st Cir. 1979) 34
Orkin Exterminating Co. v. FTC,
849 F.2d 1354 (11th Cir. 1988) 31
Papasan v. Allain,
478 U.S. 265 (1986) 26
Parke, Davis & Co. v. Califano,
564 F.2d 1200 (6th Cir. 1977) 16
Petroleum Exploration, Inc. v. Public Service Comm'n,
304 U.S. 209 (1938) 22
POM Wonderful v. FTC,
894 F. Supp. 2d 40 (D.D.C. 2012) 17
Powers v. Ohio,
499 U.S. 400 (1991) 15
Public Serv. Comm'n of Utah v. Wycoff Co.,
344 U.S. 237 (1952) 11
Reichenberger v. Pritchard,
660 F.2d 280 (7th Cir. 1981) 34
Reliable Automatic Sprinkler Co., Inc. v.
Consumer Prod. Safety Comm'n,
324 F.3d 726 (D.C. Cir. 2003) 22
Sackett v. EPA,
132 S. Ct. 1367 (2012) 23
S.C. Bd. of Dentistry v. FTC,
455 F.3d 436 (4th Cir. 2006) 16
SEC v. Chenery,
332 U.S. 194 (1947) 35

Siegel v. LePore,
234 F.3d 1163 (11th Cir. 2000) 47
Slattery v. Swiss Reinsurance Am. Corp.,
248 F.3d 87 (2d Cir. 2001) 45
Snow v. DirecTV, Inc.,
450 F.3d 1314 (11th Cir. 2006) 26
Swanson v. General Services Admin.,
110 F.3d 1180 (5th Cir. 1997) 45
Sweet Pea Marine, Ltd. v. APJ Marine, Inc.,
411 F.3d 1242 (11th Cir. 2005) 10
Tellabs, Inc. v. Makor Issues & Rights, Ltd.,
551 U.S. 308 (2007) 26
Texas v. United States,
523 U.S. 296 (1998) 17, 18, 19
Thunder Basin Coal Co. v. Reich,
510 U.S. 200 (1994) 11, 13
Ticor Title Ins. Co. v. FTC,
814 F.2d 731 (D.C. Cir. 1987) 24
Trans Union Corp. v. FTC,
245 F.3d 809 (D.C. Cir. 2001) 37
Trudeau v. FTC,
456 F.3d 178 (D.C. Cir. 2006) 24
TVA v. Whitman,
336 F.3d 1236 (11th Cir. 2003) 23, 25
Ukiah Valley Med. Ctr v. FTC,
911 F.2d 261 (9th Cir. 1990) 24

United Food & Commercial Workers Union v. Brown Grp., Inc.,
517 U.S. 544 (1996) 15
United States v. Alcon Labs.,
636 F.2d 876 (1st Cir. 1981) 16
United States v. Armstrong,
517 U.S. 456 (1996) 46
Universal Camera Corp. v. NLRB,
340 U.S. 474 (1951) 42
Varnadore v. Sec'y of Labor,
141 F.3d 625 (6th Cir. 1998) 42
Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.,
455 U.S. 489 (1982) 38
Withrow v. Larkin,
421 U.S. 35 (1975) 40, 41

FEDERAL STATUTES

5 U.S.C. § 552(a)(1) 32, 33
5 U.S.C. § 554 41
5 U.S.C. § 554(d) 8, 41
5 U.S.C. § 554(e) 41
5 U.S.C. § 556 ..... 8, 41
5 U.S.C. § 556(b) 41
5 U.S.C. § 557 9
5 U.S.C. § 557(b) 9, 42
5 U.S.C. § 702 41
5 U.S.C. § 704 20
15 U.S.C. § 45 48

15 U.S.C. § 45(a) 3, 30
15 U.S.C. § 45(b) 5, 7, 12, 42
15 U.S.C. § 45(c) ..... passim
15 U.S.C. § 45(d) 9, 14
15 U.S.C. § 45(g)-(i) 13
15 U.S.C. § 45(m)(1)(B) 32
15 U.S.C. § 45(n) ..... passim
28 U.S.C. § 1331 13
28 U.S.C. § 2201 11

FEDERAL RULES

Fed. R. Civ. P. 12(b)(1) 10, 17
Fed. R. Civ. P. 12(b)(6) ..... passim

FEDERAL REGULATIONS

16 C.F.R. § 3.22 (2008) 40
16 C.F.R. § 3.22(a) 40
16 C.F.R. § 3.44(a) (2008) 40
16 C.F.R. § 3.51 9
16 C.F.R. § 4.7(b) 8, 41
16 C.F.R. §§ 3.41-3.42 8
16 C.F.R. §§ 3.52-3.54 9
16 C.F.R. Pt. 3 ..... 7, 40
16 C.F.R. Pt. 4 40
45 C.F.R. § 160.203(b) 28
68 Fed. Reg. at 8355 28
74 Fed. Reg. 1804 (Jan. 13, 2009) 40

INTRODUCTION

LabMD asks this Court to block an ongoing adjudicatory proceeding before the Federal Trade Commission. The Federal Trade Commission ("FTC") has charged LabMD with violating the Federal Trade Commission Act ("FTC Act") by failing to protect consumers from disclosure of their sensitive personal information. LabMD may present all of its legal and factual defenses before the agency, and when the proceeding is over it may then seek judicial review of any adverse determination.

Nevertheless, LabMD has spent the past four months shopping for a court that will interrupt the administrative process, disrupt Congress's carefully crafted regime for FTC adjudications, and enjoin the pending proceeding. This Court is LabMD's third stop in its attempt to circumvent the statutory administrative and judicial review process – and the third time is not the charm. LabMD has consumed enough time and judicial resources; this Court should reject out of hand its request for a preliminary injunction, dismiss its case, and allow the orderly completion of the pending administrative process as Congress intended.

Congress set forth a comprehensive regime for the conduct and judicial review of FTC adjudicative proceedings. To date, the agency has neither compelled LabMD to do anything nor ordered it to stop any conduct. Should the Commission do so, LabMD will be entitled to judicial review of that decision. In the meantime, the Supreme Court has warned against "turning [the] prosecutor into defendant before adjudication concludes." *FTC v.*

Standard Oil, 449 U.S. 232, 243 (1980). The law is clear that this Court lacks jurisdiction to derail the legislatively established process. That is the case even though the Commission determined, in denying a motion to dismiss at the administrative level, that it has authority over data security practices.

Because the Court lacks jurisdiction, it need not reach the merits of LabMD's challenges. But they are groundless in any event. The FTC Act grants the Commission broad authority that easily encompasses harm to consumers from the release of their sensitive personal information. The Commission may exercise that authority through individual adjudications; there is no requirement that it promulgate rules prior to enforcement. FTC authority can easily co-exist with medical privacy statutes administered by the Department of Health and Human Services ("HHS"), as HHS has explicitly recognized. Indeed, today, the District Court for the District of New Jersey issued an opinion in *FTC v. Wyndham Worldwide Corp.*, No. 13-1887 Slip Op. (April 7, 2014) (attached as Ex. 8), holding that the FTC Act confers on the FTC authority over data security practices and that other statutes that also address data security do not impliedly preempt the FTC Act.

Given the Court's lack of jurisdiction and the strong likelihood that LabMD's meritless challenge will fail, the Court should deny the motion for a preliminary injunction. As LabMD's delay in filing this case shows, there is no urgency. Nor does any harm result from the administrative proceeding beyond "the expense and annoyance of litigation," which the Supreme Court

held does not constitute irreparable harm but is simply "part of the social burden of living under government." *Standard Oil*, 449 U.S. at 244.

BACKGROUND

I. Legal framework

Section 5 of the FTC Act broadly "empower[s] and direct[s]" the Commission "to prevent persons . . . from using . . . unfair . . . acts or practices in or affecting commerce." 15 U.S.C. § 45(a). As a part of an enforcement action or rulemaking proceeding, the Commission has authority to determine that an act or practice is "unfair" if that act or practice "[1] causes or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n).

Pursuant to this authority, "[t]he Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace." *See* FTC Report to Congress, Privacy Online, at 2 (June 1998) (attached as FTC Ex. 1). For well over a decade, the Commission has taken the position that the failure to maintain reasonable and appropriate data security measures constitutes an unfair act or practice in violation of Section 5. *See* Order Denying Respondent LabMD's Motion to Dismiss, FTC Dkt. No. 9357, at 8 (Jan. 16, 2014) (hereinafter "Comm'n MTD Denial") (N.D. Ga. Compl. Ex 2). It has brought "administrative adjudicatory proceedings and cases in federal court challenging practices that compromised the security of consumers' data and resulted in improper disclosures of personal

information collected from consumers online." *Id.* A similar ongoing administrative adjudicatory proceeding against LabMD is the subject of the suit before this Court.

II. The administrative investigation and complaint

LabMD, a Georgia-based medical testing company, conducted clinical laboratory tests on specimen samples from consumers throughout the United States. *See* Complaint, FTC Dkt. No. 9357 (Aug. 28, 2013) (hereinafter "Admin. Compl.") (N.D. Ga Compl. Ex. 4). In 2009, the FTC learned that sensitive personal information in LabMD's possession had been made available to the public on peer-to-peer file sharing networks. N.D. Ga. Compl. Ex. 8 at 2. The FTC staff undertook an investigation into LabMD's data security practices beginning in early 2010. *See* Compl. ("N.D. Ga. Compl.") ¶ 10 (ECF No. 1). The investigation culminated in a Commission determination that there was "reason to believe" that LabMD may have engaged in unfair acts or practices in violation of Section 5 of the FTC Act by failing to maintain reasonable data security practices. *See* Admin. Compl., Preamble (quoting 15 U.S.C. § 45(b)). The Commission determined further that an administrative adjudication of these allegations would be in the public interest. *Id.*

Accordingly, on August 28, 2013, the Commission issued the administrative complaint against LabMD. The complaint alleges that LabMD has accumulated and maintained personal information (such as date of birth, social security numbers, medical information, and bank account or

credit card information) on nearly one million consumers. Admin. Compl. ¶¶ 6-7. In spite of the sensitivity and volume of consumer data that it stores, the company allegedly did not implement or maintain a comprehensive data security program to protect that data; did not use readily available technology to identify commonly known or reasonably foreseeable security risks and vulnerabilities to the security of this data; did not use appropriate measures to prevent employees from accessing consumers' 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 consumers' personal information. *Id.* ¶ 10. The administrative complaint alleges that, taken together, these practices constitute a failure to provide reasonable and appropriate security for personal information on LabMD's computer networks. *Id.* It further alleges that while LabMD could have corrected its problematic practices "at relatively low cost using readily available security measures," consumers harmed by LabMD's security failures could not have taken steps to protect themselves from such harm because "consumers have no way of independently knowing about" them. *Id.* ¶¶ 11-12.

The administrative complaint discusses one example of LabMD's data security failures: the company allegedly failed to detect that its billing manager had installed Limewire, a peer-to-peer file sharing application, on a LabMD computer. *Id.* ¶¶ 10(g), 18(a). Peer-to-peer 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 also be shared inadvertently. Once a file has been made available on a peer-to-peer 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. *See* Admin. Compl. ¶¶ 13-16. A third party informed LabMD that a LabMD file containing sensitive information about thousands of consumers was available on a P2P network through Limewire. *Id.* ¶ 17; *see also* Compl. ¶ 3, *LabMD v. FTC,* No. 1:13-cv-1787 (Nov. 14, 2013 D.D.C.) ("D.C. Compl.") (FTC Ex. 2).[1] Hundreds of other files from the billing manager's computer allegedly were also designated for sharing on Limewire. Admin. Compl. ¶ 18.

The administrative complaint recounts an additional security incident, which illustrates the potential for consumer injury resulting from the unauthorized disclosure of consumers' information collected by LabMD. Sacramento police found different LabMD documents containing personal information from hundreds of consumers in the possession of identity thieves. *Id.* ¶ 21. LabMD's alleged failure to maintain reasonable security measures elevates the risk of consumer harm. *See id.* ¶ 10.

[1] That file contained personal information on approximately 9,300 consumers, including their names, dates of birth, social security numbers, information about laboratory tests run, and, in many instances, their health insurance company names, addresses, and policy numbers. Admin. Compl. ¶ 19.

The administrative process is underway. Once the Commission voted out the complaint, it was referred to an administrative law judge ("ALJ"). No remedy may be imposed until the conclusion of the administrative adjudicatory proceeding before the ALJ, *see* 15 U.S.C. § 45(b) (authorizing and governing FTC adjudicatory proceedings); 16 C.F.R. Pt. 3 (rules of practice and procedure governing such cases).

Shortly after the adjudicatory proceeding began, LabMD moved to dismiss the complaint before the Commission. The Commission denied the motion, holding that the complaint concerned matters within the FTC's authority and the agency had not violated LabMD's right to due process. *See* Comm'n MTD Denial at 18-19. The Commission explained further that its "ultimate decision on LabMD's liability will depend on the factual evidence to be adduced in this administrative proceeding." *Id.* at 18. For example, the Commission would need to determine not only "whether the facts alleged in the Complaint actually occurred, but also whether LabMD's data security procedures were 'unreasonable' in light of the circumstances." *Id.*

Accordingly, the matter is now before the ALJ, the parties have been conducting discovery, and the evidentiary hearing is set to begin on May 20, 2014. *See* Comm'n MTD Denial at 2. At the hearing, LabMD and the Commission's enforcement staff ("complaint counsel")[2] will present evidence

[2] To ensure separation of the Commission's prosecutorial and adjudicatory roles, complaint counsel remains "walled off" from the Commission for the duration of the proceeding, as required by the Administrative Procedure Act ("APA"). *See* 5 U.S.C. § 554(d); 16 C.F.R. § 4.7(b).

and legal argument to the ALJ. *See* 16 C.F.R. §§ 3.41-3.42. *Cf.* 5 U.S.C. §§ 554(d), 556. LabMD will have the opportunity to refute complaint counsel's evidence and argument, and to present evidence and argument of its own. The ALJ will then issue an "initial decision" containing findings of fact and conclusions of law. 16 C.F.R. § 3.51; *cf.* 5 U.S.C. § 557.

Either LabMD or complaint counsel may appeal the ALJ's initial decision to the full Commission, which would conduct a *de novo* review of both the factual findings and legal conclusions in the ALJ's initial decision. 16 C.F.R. §§ 3.52-3.54; 5 U.S.C. § 557(b). If, after reviewing the record, the Commission determines that LabMD has engaged in "unfair acts or practices" and enters a final order to cease and desist, then LabMD "may obtain a review of such order in the court of appeals," 15 U.S.C. § 45(c), which has "exclusive" jurisdiction "to affirm, enforce, modify, or set aside" the Commission's order, *id* § 45(d).

III. LabMD's multiple federal court challenges to the ongoing administrative proceedings

LabMD has sought to disrupt the enforcement proceeding against it in three different forums. A week after filing its motion to dismiss before the FTC, LabMD filed a complaint against the FTC in the U.S. District Court for the District of Columbia. Four days later, it filed a petition for review in the Eleventh Circuit. While the district court case was pending, the Eleventh Circuit dismissed its case for lack of jurisdiction. N.D. Ga. Compl. Ex. 1. If any court had jurisdiction, the Eleventh Circuit suggested, it would be a

district court, although the court did not "express or imply any opinion about whether a district court has jurisdiction to hear such claims or about the merits of those claims." *Id.* at 2. Yet even though LabMD had a district court case pending in D.C., it dismissed that case. *See* Notice of Voluntary Dismissal, *LabMD v. FTC,* No. 1:13-cv-1787 (Feb. 19, 2014 D.D.C.) (FTC Ex. 3). More than a month later, it filed the instant case – and a motion for emergency relief that it had not asked for in D.C.[3] In each proceeding, the essence of LabMD's claims has remained the same.

ARGUMENT

I. The complaint must be dismissed for lack of jurisdiction

"The burden for establishing federal subject matter jurisdiction rests with the party bringing the claim." *Sweet Pea Marine, Ltd. v. APJ Marine, Inc.*, 411 F.3d 1242, 1247 (11th Cir. 2005). Pursuant to Fed. R. Civ. P. 12(b)(1), the district court is not limited to considering the complaint alone, but may also consider facts in the record. *McElmurray v. Consol. Gov't*

[3] This Court previously heard a related case in 2012, before the administrative complaint was issued. There, the FTC served several civil investigative demands on Michael Daugherty and LabMD. When they refused to comply, the Commission sought an order from this Court to enforce the civil investigative demands. *See* N.D. Ga. Compl. Ex. 8. In response, they argued that the FTC lacked the authority to investigate and bring enforcement actions with respect to data security issues, and that the FTC had been divested of jurisdiction to regulate data security by laws governing health information. Opp'n Brief, *FTC v. LabMD*, No. 1:12-cv-03005-WSD, at 17 (N.D. Ga. Sept. 14, 2012) (FTC Ex. 4). The Court rejected these arguments, explaining that the FTC had made "a plausible argument in support of its assertion of jurisdiction" over data security issues. N.D. Ga. Compl. Ex. 8.

Augusta–Richmond Cnty, 501 F.3d 1244, 1251 (11th Cir. 2007). Absent subject matter jurisdiction, a court may not order injunctive or declaratory relief. 28 U.S.C. § 2201 ("In a case of *actual controversy* within its jurisdiction . . . any court . . . may declare the rights. . . ." (emphasis added)); *Public Serv. Comm'n of Utah v. Wycoff Co.*, 344 U.S. 237, 242 (1952). LabMD cannot show that this – or any other – federal court has jurisdiction to entertain any of LabMD's claims at this time.

A. This Court lacks jurisdiction to consider any of LabMD's claims because doing so would interfere with the ongoing FTC proceeding

Two separate lines of Supreme Court precedent make clear that plaintiff cannot invoke the jurisdiction of this Court to interfere with the ongoing FTC proceeding against it. In *Thunder Basin Coal Co. v. Reich*, 510 U.S. 200, 207-08 (1994), the Supreme Court explained that federal courts lack jurisdiction to consider any *claims* related to an ongoing administrative adjudication when – as is the case here – Congress intended to foreclose interlocutory review. And in the *Ewing v. Mytinger & Casselberry, Inc.*, 339 U.S. 594, 598 (1950) line of cases, the Supreme Court made clear that the type of *relief* plaintiff seeks – enjoining ongoing administrative proceedings – is not available from any federal court.

1. This Court lacks jurisdiction over pre-enforcement challenges to an administrative adjudication

Congress crafted a detailed regime for administrative adjudication of complaints and provided an exclusive means for challenging a final order resulting from an FTC administrative proceeding. The FTC Act specifies that, upon finding "reason to believe" that any person has engaged in "unfair or deceptive act or practice in or affecting commerce," the Commission may undertake an adjudication to determine if such acts were committed. 15 U.S.C. § 45(b). Congress laid out in some detail how that process should proceed, including judicial review. *Id.* Importantly, Congress vested the court of appeals with exclusive jurisdiction to review any final agency cease-and-desist order. *Id.* § 45(c).

LabMD does not challenge a final Commission cease-and-desist order; no such order has been issued. *See* N.D. Ga. Compl. ¶¶ 97, 106. Rather, it challenges a pending administrative complaint and an interlocutory agency order denying a motion to dismiss that complaint. LabMD may raise before the FTC all the claims it raises here. Although the Commission has rejected some of those defenses and arguments, neither the administrative law judge overseeing the proceeding nor the Commission has determined LabMD's liability under the FTC Act. *See* Comm'n MTD Denial.

Where Congress has provided "a detailed structure for reviewing violations" of a statute and granted to the court of appeals exclusive jurisdiction to review administrative decisions resulting from that process,

those legislative requirements "demonstrate[] that Congress intended to preclude challenges" prior to the completion of agency proceedings. *Thunder Basin*, 510 U.S. at 207-208. Thus, a district court is "preclude[d] [from] . . . exercising jurisdiction over [a] pre-enforcement challenge" to agency proceedings. *Id.* at 216. The FTC Act is the same type of statutory regime as that in *Thunder Basin*. The Supreme Court explained that judicial intervention prior to the conclusion of the administrative process was precluded because such premature judicial review would be tantamount to "evad[ing] the statutory-review process." *Id.*[4]

Here, the detailed procedures specified in the FTC Act, *see* 15 U.S.C. § 45(c), (g)-(i), provide a full opportunity for LabMD to obtain judicial review. Where, as here, "Congress has provided an adequate procedure for judicial review of administrative action, that procedure must be followed." *Frito-Lay, Inc. v. FTC*, 380 F.2d 8, 10 (5th Cir. 1967) (per curiam). LabMD is flatly wrong when it contends that under the FTC Act a "district court has jurisdiction until [a final order] has been issued." *See* Pl.'s PI Mem. at 12 (ECF No. 2). The FTC Act provides that *the FTC* and the court of appeals have concurrent jurisdiction until the administrative record is filed with the court. 15 U.S.C. § 45(c), (d). Those provisions say nothing about district court jurisdiction, which would be wholly inconsistent with Congress's grant

[4] The statutory review process laid out in the FTC Act precludes the exercise of jurisdiction over not only an APA claim, but also a constitutional challenge brought in district court pursuant to 28 U.S.C. § 1331. *See Elgin v. Dept. of Treasury*, 132 S. Ct. 2126, 2132-33 (2012).

of "exclusive" jurisdiction to the court of appeals. Congress's chosen regime for review of FTC proceedings makes clear that, until the FTC issues a final order, LabMD must raise its arguments before the agency and may not seek a judicial injunction to sidestep the legislatively mandated administrative process. LabMD will have a full opportunity for review of any adverse result, including review of the Commission's jurisdiction over data security practices. *See* 15 U.S.C. § 45(c)-(d). The Eleventh Circuit's order dismissing LabMD's earlier challenges in that court does not suggest otherwise. Indeed, the court of appeals pointedly did not "express or imply any opinion about whether a district court has jurisdiction to hear such claims or about the merits of those claims." N.D. Ga. Compl. Ex. 1.

The prohibition on invoking the judicial process to nullify the administrative process remains in effect when the FTC has denied a motion to dismiss the administrative complaint. So long as LabMD is entitled to full judicial review at the conclusion of the proceeding – which under the FTC Act it is – it may not "turn[] [the] prosecutor into defendant before adjudication concludes." *Standard Oil*, 449 U.S. at 243.

2. This Court cannot enjoin the ongoing administrative proceedings

LabMD's complaint also must be dismissed in its entirety because district courts lack jurisdiction to enjoin ongoing administrative enforcement

proceedings.[5] The Supreme Court established long ago that having a court separate from the enforcement action enjoin ongoing administrative proceedings would result in unnecessary and premature judicial interference. *See Ewing*, 339 U.S. at 598; *Myers v. Bethlehem Shipbuilding Corp.*, 303 U.S. 41, 48 (1938) ("The District Court is without jurisdiction to enjoin [NLRB's administrative] hearings[.]"). The Court explained that "it has never been held that the hand of government must be stayed until the courts have an opportunity to determine whether the government is justified in instituting suit." *Ewing*, 339 U.S. at 599. Since that time, that principle has been "consistently and strictly observed" by courts throughout the country. *United States v. Alcon Labs.*, 636 F.2d 876, 881-82 (1st Cir. 1981) (the issuance of preemptive injunctive relief "might seriously impair the effectiveness of the Act's enforcement provisions"); *see, e.g.*, *Parke, Davis & Co. v. Califano*, 564 F.2d 1200, 1206 (6th Cir. 1977) ("[I]t was an abuse of discretion to enjoin the [agency] . . . where pending enforcement actions provided an opportunity for a full hearing before a court."). *Cf. N.C. Bd. Dental Examiners v. FTC*, 768 F. Supp. 2d 818, 822 (E.D.N.C. 2011) ("Where the instant lawsuit seeks a

[5] LabMD's request that the Court block FTC enforcement actions against third parties, N.D. Ga. Comp. ¶ 135, runs afoul of "the general prohibition on a litigant's raising another person's legal rights." *United Food & Commercial Workers Union Local 751 v. Brown Grp., Inc.*, 517 U.S. 544, 557 (1996) (quotation omitted). LabMD alleges no "close relation" between it and any third party or any "hindrance to the third party's ability to protect his or her own interests" that would warrant third party standing. *Powers v. Ohio*, 499 U.S. 400, 411 (1991). Accordingly, the request for this type of relief must be dismissed for lack of jurisdiction.

declaration that defendant's litigating position in the administrative proceedings is contrary to law . . . its unmistakable purpose and effect is to short-circuit [*Ewing*]."); *accord S.C. Bd. of Dentistry v. FTC*, 455 F.3d 436 (4th Cir. 2006).

Indeed, courts have found *Ewing* to bar federal courts from exercising jurisdiction over actions to enjoin FTC adjudicative proceedings, even in the face of constitutional and jurisdictional challenges like those plaintiff raises here. *See, e.g.*, *N.C. Bd. Dental Examiners*, 768 F. Supp. 2d 818 (dismissing plaintiff's claims for declaratory and injunctive relief arising from ongoing administrative proceeding initiated by the FTC, despite allegations that the FTC's proceedings exceeded the agency's jurisdiction); *Direct Mktg. Concepts, Inc. v. FTC*, 581 F. Supp. 2d 115, 117 (D. Mass. 2008) ("Any challenges to the propriety of the agency action [including a First Amendment claim] should be addressed in the enforcement action itself."); *POM Wonderful v. FTC*, 894 F. Supp. 2d 40, 44 (D.D.C. 2012) ("[The FTC] is 'perfectly capable' of determining whether [administrative action] exceeds the bounds of the FTC Act [or] violates the First and Fifth Amendments."). Because this Court does not have the power to issue the relief LabMD seeks, the complaint must be dismissed in its entirety.

B. LabMD's claims are all patently unripe

Any unripe claims must be dismissed pursuant to Rule 12(b)(1). *See Digital Properties, Inc. v. City of Plantation*, 121 F.3d 586, 589 (11th Cir. 1997). "A claim is not ripe for adjudication if it rests upon contingent future

events that may not occur as anticipated, or indeed may not occur at all." *Texas v. United States*, 523 U.S. 296, 300 (1998) (quotation omitted).

LabMD's claims are unripe because they depend on the occurrence of far-from-certain contingencies. At this point, it is impossible to know how the FTC will resolve this matter. Depending on the record developed at trial, the administrative proceedings may resolve in LabMD's favor. Before making a final determination, the FTC will "need to determine . . . not only whether the facts alleged in the Complaint actually occurred, but also whether LabMD's data security procedures were 'unreasonable' in light of the circumstances. Whether LabMD's security practices were unreasonable is a factual question that can be addressed only on the basis of evidence to be adduced in [the administrative adjudicatory] proceeding." Comm'n MTD Denial at 18-19.

This is *exactly* the kind of case where the ripeness doctrine should "prevent the courts, through avoidance of premature adjudication, from entangling themselves in abstract disagreements over administrative policies, and also . . . protect the agencies from judicial interference until an administrative decision has been formalized and its effects felt in a concrete way by the challenging parties." *Ohio Forestry Ass'n v. Sierra Club*, 523 U.S. 726, 732-33 (1998) (citation omitted). Indeed, in *Texas v. United States*, the Supreme Court upheld the dismissal of an analogous case on ripeness grounds. There, plaintiff sought a declaratory judgment that would have blocked a proceeding pending before the Department of Justice to determine whether Texas had violated the Voting Rights Act. 523 U.S. at 300. Just as

LabMD claims here, Texas claimed that the statute did not apply to its conduct. The Court held the case was not ripe because:

> The operation of the statute is better grasped when viewed in light of a particular application. Here, as is often true, "[d]etermination of the scope . . . of legislation in advance of its immediate adverse effect in the context of a concrete case involves too remote and abstract an inquiry for the proper exercise of the judicial function."

Id. at 301 (quoting *Longshoremen v. Boyd*, 347 U.S. 222, 224 (1954)).

LabMD suggests that this case is ripe because the FTC has somehow "predetermined" its outcome. N.D. Ga. Compl. ¶¶ 106, 142. However, plaintiff does not allege that the administrative proceedings have resolved all contested issues of fact, let alone whether LabMD violated the FTC Act at all. *See id.* Nor is LabMD correct that the Commission votes in favor of complaint counsel in every instance. *See* N.D. Ga. Compl. ¶ 94. For example, earlier this year, the Commission issued an opinion in an adjudicatory case, reversing the ALJ's rulings holding the respondent liable on certain counts in the complaint, and instead concluded that Complaint Counsel had failed to establish that the respondent's conduct was unlawful. *See In re McWane, Inc., and Star Pipe Products, Ltd.*, FTC Docket No. 9351, Opinion of the Commission (January 30, 2014) (FTC Ex. 5).[6]

[6] LabMD's further suggestion that Commissioner Brill's involvement in the case means the case has been "predetermined" is also entirely without merit. *See* N.D. Ga. Compl. ¶¶ 29-32. Commissioner Brill has recused herself from ongoing proceedings in the underlying administrative matter. *See* Statement of Comm'r Brill, FTC Dkt. No. 9357 (Dec. 24, 2013) (FTC Ex. 6).

C. The Court lacks jurisdiction over plaintiff's APA claim, which does not challenge final agency action

LabMD's first claim for relief seeks redress for alleged APA violations. In addition to the reasons discussed above why the entire complaint must be dismissed for lack of jurisdiction, LabMD's first claim suffers from another fatal flaw: it fails to challenge final agency action because none has occurred.

The APA permits judicial review of "[a]gency action made reviewable by statute and *final agency action* for which there is no other adequate remedy in a court." 5 U.S.C. § 704 (emphasis added). It is well-established that, except as otherwise provided by statute,[7] "[i]f the agency action is not final, the court" lacks "federal subject matter jurisdiction." *Nat'l Parks Conservation Ass'n v. Norton*, 324 F.3d 1229, 1236, 1240 (11th Cir. 2003). None of the actions plaintiff challenges under the APA – the filing of the administrative complaint, the inclusion of a proposed remedy, or the denial of LabMD's motions to dismiss and for a stay, *see* N.D. Ga. Compl. ¶¶ 104-106 – constitutes final agency action.

The Supreme Court has held squarely that the FTC's issuance of an administrative complaint is not final agency action subject to judicial review. *Standard Oil*, 449 U.S. 232. To the contrary, an FTC complaint "represents a threshold determination that further inquiry is warranted and that a

[7] LabMD does not claim it is seeking judicial review of an action "made reviewable by statute" – nor could it because, as discussed *supra* Part I.A.1, the FTC Act grants a right of review only for final FTC cease and desist orders and even then vests exclusive review in the court of appeals.

complaint should initiate proceedings." *Id.* at 241. The Court made clear that a complaint is not a final action even though it is "definitive" on the question regarding whether the Commission had "reason to believe" that the respondent violated the FTC Act. *Id.* The Court warned in particular against judicial "interference with the proper functioning of the agency," which "denies the agency an opportunity to . . . apply its expertise." *Id.* at 242. Because an administrative complaint is not final agency action, a remedy proposed in such a complaint *a fortiori* cannot be final agency action.

Under *Standard Oil*, the FTC's denial of a motion to dismiss also is not final agency action, even when the Commission's denial rejects an argument that the Commission has exceeded its statutory authority. *Standard Oil*, 449 U.S. at 243. As here, Standard Oil had filed a motion to dismiss an FTC administrative adjudication, *id.* at 235 n.5, and a motion for reconsideration, *id.* at 241 n.9. The Commission had denied both of Standard Oil's motions. Even though Standard Oil had no further administrative opportunity to challenge issuance of the complaint, the Supreme Court concluded that judicial review was premature. As the Court explained, to hold otherwise would "mistake[] exhaustion for finality." In filing an administrative motion to dismiss:

> [Plaintiff] may well have exhausted its administrative remedy as to the averment [that the Commission has] reason to believe [an FTC act violation occurred]. But the Commission's refusal to reconsider its issuance of the complaint does not render the complaint a "definitive" action. The Commission's refusal does not augment the complaint's legal force or practical effect upon

> [plaintiff]. Nor does the refusal diminish the concerns for efficiency and enforcement of the Act.

Id.; *see also Reliable Automatic Sprinkler Co., Inc. v. Consumer Prod. Safety Comm'n*, 324 F.3d 726, 733 (D.C. Cir. 2003) ("The policy undergirding the finality requirement is no less applicable to piecemeal appeals on issues of statutory authority than to piecemeal appeals on other points." (quotation omitted)). That rationale applies equally to the Commission's denial of LabMD's motion for a stay.

The Supreme Court recognized in *Standard Oil* that requiring regulated parties to complete the administrative process would impose a burden on them. "[T]he expense and annoyance of litigation is 'part of the social burden of living under government.'" 449 U.S. at 244 (quoting *Petroleum Exploration, Inc. v. Public Service Comm'n*, 304 U.S. 209, 222 (1938)). But "mere litigation expense, even substantial and unrecoupable cost, does not constitute irreparable injury." *Id.*

Despite plaintiff's suggestion, neither the Supreme Court nor the Eleventh Circuit has retreated from *Standard Oil*'s unambiguous holding that the FTC's filing of an administrative complaint or denial of a motion to dismiss does not constitute final agency action. *See* N.D. Ga. Compl. ¶106. The cases relied on by LabMD show no such thing. In *TVA v. Whitman*, 336 F.3d 1236, 1239 (11th Cir. 2003), the Eleventh Circuit found that "legally inconsequential" agency decisions are not final agency action subject to review – which in no way abrogates *Standard Oil*. In *Sackett v. EPA*, the Supreme Court found final agency action where the EPA's order imposed on

the Sacketts the *immediate* "legal obligation to 'restore' their property according to an agency-approved Restoration Work Plan, and [to] give the EPA access to their property." 132 S. Ct. 1367, 1371 (2012). By contrast, the Commission's denial of LabMD's motion to dismiss does not require the company to do *anything*, aside from continue with the administrative process.

Nor do the other, non-binding cases that plaintiff cites call the *Standard Oil* rule into question. *See* N.D. Ga. Compl. ¶106. In *CSI Aviation Servs. v. US Dep't of Transportation*, 637 F.3d 408 (D.C. Cir. 2011), the agency had issued a cease-and-desist letter that effectively required immediate compliance and was not "subject to further agency consideration or possible modification." *Id*. at 412. Moreover, there were no "disputed facts that would bear on" whether the company had violated the law. *Id*. No such factors are present here. *Athlone Indus. Inc. v. Consumer Prod. Safety Comm'n*, 707 F.2d 1485 (D.C. Cir. 1983), addressed exhaustion, not finality – the very distinction recognized in *Standard Oil* as dispositive. *See Ukiah Valley Med. Ctr v. FTC*, 911 F.2d 261, 266 (9th Cir. 1990) (explaining that *Athlone* dealt with exhaustion and not finality). *Trudeau v. FTC*, 456 F.3d 178 (D.C. Cir. 2006), is inapposite because it involved review of an FTC press release that, unlike an administrative complaint, was not reviewable under the ordinary FTC judicial review provisions.

The FTC has argued in other litigation that deference under *Chevron v. NRDC*, 467 U.S. 837 (1984), applies to its construction of Section 5 of the FTC Act in the order denying LabMD's motion to dismiss. *See* N.D. Ga. Compl.

Ex. 6. Contrary to LabMD's contention, that position does not render the LabMD proceeding final. The Commission's ruling represents a definitive interpretation of the application of Section 5 to data security, but as the Supreme Court held in *Standard Oil*, that does not make the proceeding final under the APA.

Even if *Standard Oil* did not definitively resolve the matter, the Court should also consider whether the action affects the legal rights and obligations of the parties; whether the action will have an immediate impact on the daily operations of the regulated party; whether pure questions of law are involved; and whether pre-enforcement review will be efficient. *See TVA*, 336 F.3d at 1248. None of those factors are pertinent here. The FTC's denial of LabMD's motion to dismiss does not affect LabMD's legal rights and obligations and will not have an impact on LabMD's daily operation because it does not resolve whether LabMD's data security practices are unreasonable or require any action or inaction on LabMD's part. Comm'n MTD Denial at 18-19. Nor does this matter involve "pure questions of law." Substantial facts must be resolved before the ALJ and the FTC can assess whether LabMD has violated Section 5. For the same reason, judicial review at this point would be inefficient because it would prevent the FTC from even examining LabMD's conduct. *See Ohio Forestry*, 523 U.S. at 732-33.

II. In the alternative, the complaint should be dismissed for failure to state a claim

Because the Court lacks jurisdiction over the complaint for the foregoing reasons, it need not proceed further. Should it determine that it has jurisdiction, however, the Court should dismiss the complaint because it "fail[s] to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). "[A] complaint [does not] suffice if it tenders 'naked assertion[s]' devoid of 'further factual enhancement.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007)). Instead, a valid complaint contains sufficient factual allegations that, if accepted as true, "state a claim to relief that is plausible on its face." *Twombly*, 550 U.S. at 570. A claim is plausible on its face only if "the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. The Court is "not bound to accept as true a legal conclusion couched as a factual allegation," *Papasan v. Allain*, 478 U.S. 265, 286 (1986), or to "accept inferences drawn by plaintiffs if such inferences are unsupported by the facts set out in the complaint," *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1320 (11th Cir. 2006) (citation omitted). In evaluating a Rule 12(b)(6) motion, the Court may consider facts contained in any attachments to, or documents incorporated into, the complaint. *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007). Even if the Court otherwise

had jurisdiction in this case – which it does not – none of plaintiff's claims for relief survive the 12(b)(6) standard.

A. Plaintiff fails to state a valid claim that the FTC lacks power to regulate data security

LabMD claims that the FTC lacks authority to regulate data security because Section 5 of the FTC Act says nothing about data security. *See* N.D. Ga. Compl. ¶¶ 104, 118. Plaintiff also claims that Congress divested any possible FTC authority over data security in the health field when it passed the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which HHS administers. *Id* ¶¶ 104, 118.[8] Neither of these arguments states a valid claim.

There is no validity to plaintiff's argument that HIPAA and HITECH divest the FTC of otherwise applicable Section 5 authority. To be sure, HIPAA and HITECH address the security of health data. But "[w]hen [multiple] statutes are capable of coexistence, it is the duty of the courts, absent a clearly expressed congressional intention to the contrary, to regard each as effective." *J.E.M. Ag. Supply, Inc. v. Pioneer Hi-Bred Int'l, Inc.*, 534 U.S. 124, 143-44 (2001); *see also* Comm'n MTD Denial at 10-13. The FTC

[8] LabMD further claims that "[n]either the HHS nor the FTC has accused LabMD of violating HIPAA or HITECH." N.D. Ga. Compl. ¶ 17. The FTC, which does not enforce either of those statutes, has never expressed any view on whether LabMD has, or has not, violated those statutes – or whether it is subject to regulation under any statute beyond the FTC Act.

Act, HIPAA, and HITECH clearly are consistent with one another, and Congress wanted sensitive personal health information to be protected under both regimes. *See* Comm'n MTD Denial at 11-14.[9] LabMD contends in effect that HIPAA and HITECH impliedly repealed the FTC's Section 5 authority, but "[a]n implied repeal will only be found where provisions in two statutes are in 'irreconcilable conflict,' or where the [later] Act covers the whole subject of the earlier one and 'is clearly intended as a substitute.'" *Id.* at 11 (citing *Branch v. Smith*, 538 U.S. 254, 273 (2003)).

That is clearly not the case here. Neither HIPAA nor HITECH forecloses the possibility that another agency plays a parallel role in protecting patient data security. Indeed, in adopting regulations implementing HIPAA, HHS stated that "[s]ecurity standards in this final rule establish a *minimum* level of security that covered entities must meet. We note that covered entities may be required by other Federal law to adhere to *additional*[] or more stringent security measures." 68 Fed. Reg. at 8355 (emphasis added).[10] Accordingly, HIPAA and HITECH authority are capable of co-existing with the FTC's authority to police unfair consumer practices in the area of patient-information data-security.

---

[9] Of note, FTC and HHS have worked in tandem in previous enforcement cases, with each agency seeking complementary penalties. *See* Comm'n MTD Denial at 11.

[10] Moreover, HHS regulations provide that state laws "related to the privacy of individually identifiable health information [that are] more stringent than" HHS's requirements are not preempted. 45 C.F.R. § 160.203(b).

In the absence of any reason to believe that HIPAA and HITECH affirmatively displace FTC authority, the Commission's interpretation of Section 5 is entitled to *Chevron* deference. *City of Arlington v. FCC*, 133 S. Ct. 1863, 1868-69 (2013) (whether an agency is acting beyond the scope of its authority is a question of the agency's interpretation of its organic act). The Court explained that the agency's interpretation of its statutory jurisdiction is no different from its interpretation of any other provision of the statute it administers; rather, because the agency's "power to act and how they are to act is authoritatively prescribed by Congress," there is "no principled basis for carving out some arbitrary subset of such claims as 'jurisdictional.'" *Id.* at 1869. Here, the FTC has reasonably interpreted the FTC Act and determined that its broad grant of authority covers potentially harmful data security practices.

It is of no moment that the FTC Act does not address data security. Section 5 of the Act broadly empowers the FTC to take action against *any* "unfair . . . acts or practices in or affecting commerce," as long as 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 competition." 15 U.S.C. § 45(a), (n). Congress crafted this standard broadly to afford the Commission substantial discretion in its application. It therefore does not "delineate all of the specific 'kinds' of practices which will be deemed unfair," but allows the FTC "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 Atl. Refining Co. v. FTC*, 381 U.S. 357, 367 (1965) ("[Congress] intentionally left development of the term 'unfair' to the Commission rather than attempting to define 'the many and variable unfair practices which prevail in commerce.'") (quoting S. Rep. No. 592, 63d Cong., 2d Sess., 13 (1914)). Indeed, the Supreme Court has long held that "[n]either the language nor the history of the [FTC] [A]ct suggests that Congress intended to confine the forbidden methods to fixed and unyielding categories." *FTC v. R.F. Keppel & Bro., Inc.*, 291 U.S. 304, 310 (1934). The Commission had ample room to interpret the Act's expansive language as granting authority over data security practices. Comm'n MTD Denial at 3-5; *see also Wyndham,* Slip Op. 10-15.

Thus, federal courts have upheld Commission determinations finding a wide range of acts or practices that satisfy the applicable criteria to be "unfair" within the meaning of Section 5, even though these practices are not explicitly mentioned in Section 5. *See, e.g.*, *FTC v. Neovi, Inc.*, 604 F.3d 1150, 1155 (9th Cir. 2010) (creating unverified checks that enabled fraudsters to take unauthorized withdrawals from consumers' bank accounts); *FTC v. Accusearch, Inc.*, 570 F.3d 1187, 1193 (10th Cir. 2009) (covert retrieval and sale of consumers' telephone billing information); *Orkin Exterminating Co. v. FTC,* 849 F.2d 1354, 1364 (11th Cir. 1988) (unilateral breach of standardized service contracts). Accepting plaintiff's contrary approach would significantly hobble the FTC's ability to keep pace with ever-changing methods of consumer harm. But Congress plainly intended the Commission to have the

authority "to determine what practices were unfair" rather than "enumerating the particular practices to which [the term 'unfair'] was intended to apply." *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 240 (1972) (quoting S. Rep. No. 597, 63d Cong., 2d Sess., 13 (1914), and H.R. Conf. Rep. No.1142, 63d Cong., 2d Sess., 19 (1914)). Congress knew that there "is no limit to human inventiveness" in commerce. *Id*. Thus, "[e]ven if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again." *Id*.

This Court has already found that the Commission's interpretation of Section 5 passes deferential scrutiny, holding that the FTC had made such a showing with respect to its investigation of LabMD:

> 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.

N.D. Ga. Compl. Ex. 2 at 13. Here too, LabMD has not met its burden to show that the FTC has improperly exercised its statutory authority.

B. Plaintiff's other *ultra vires* claims also fail under 12(b)(6)

The remainder of plaintiff's claims that the FTC has exceeded its authority also fail. *See* N.D. Ga. Compl. ¶¶ 117-119. The first statute that plaintiff contends the FTC has violated, 15 U.S.C. § 45(m)(1)(B), is not at issue here. That provision addresses when "the Commission may commence a civil action to obtain a civil penalty in a district court of the United States."

But the Commission has not sued LabMD in federal court nor is it currently seeking a civil penalty from LabMD. The FTC is also not in violation of 5 U.S.C. § 552(a)(1), which *inter alia* requires agencies to publish the results of formal notice-and-comment rulemaking in the Federal Register. As plaintiff itself vigorously argues, the FTC has not adopted any rule subject to that provision, which makes § 552(a)(1) entirely irrelevant here.

The FTC has also not violated the specific limits 15 U.S.C. § 45(n) places on the agency's Section 5 unfairness authority. Under that provision, an act or practice must "cause[] or [be] 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" to be considered unfair. "In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination." *Id.* Poor data security practices surely can harm consumers, including increased vulnerability to identity theft. *See* Admin. Compl. ¶ 12. The administrative complaint alleges that LabMD could have corrected its problematic practices "at relatively low cost using readily available security measures," and that consumers could not take steps to protect themselves against harm from LabMD's security failures because "consumers have no way of independently knowing about" them. Admin. Compl. ¶¶ 11-12. If proven true by the evidence introduced at the administrative hearing, these allegations would

establish that the injury was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits. Plaintiff's claim that the FTC is using public policy as its prime motivation in bringing an enforcement action against LabMD is a "naked assertion devoid of further factual enhancement" that must be dismissed. *Iqbal*, 556 U.S. at 678.

C. Plaintiff fails to make a valid "fair notice due process" claim

1. Plaintiff's claim does not implicate a liberty or property interest

As a threshold matter, a plaintiff attempting to assert a due process claim must demonstrate that a liberty or property interest is implicated. *Bd. of Regents of State Colleges v. Roth*, 408 U.S. 564, 569 (1972). "The mere possibility of remote or speculative future injury or invasion of rights will not suffice" to meet this requirement. *Reichenberger v. Pritchard*, 660 F.2d 280, 282 (7th Cir. 1981); *see Clapper v. Amnesty Int'l, USA*, 133 S. Ct. 1138, 1147 (2013) ("threatened injury must be *certainly impending* to constitute injury in fact, and that allegations of *possible* future injury are not sufficient.").

In its third claim for relief, plaintiff alleges that its property rights are implicated because a draft order, which the Commission has not in fact entered against LabMD, *could* lead to monetary damages *if* complaint counsel prevails in front of the ALJ, the Commission upholds the determination, and LabMD takes future actions in violation of that (currently

non-existent) order. *See* N.D. Ga. Compl. ¶¶ 156-58. This chain of events is far too attenuated to implicate a cognizable liberty or property interest.

2. Due process does not require the FTC to issue data security regulations before bringing an enforcement action against LabMD

Plaintiff incorrectly contends that due process requires the FTC to issue data security regulations before bringing an enforcement action against LabMD. *See* N.D. Ga. Compl. ¶ 128. But the Supreme Court has rejected such an approach, explaining instead that:

> [Regulatory] problems may arise . . . [that] must be solved despite the absence of a relevant general rule. Or the agency may not have had sufficient experience with a particular problem to warrant rigidifying its tentative judgment into a hard and fast rule. Or the problem may be so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule. In those situations, the agency must retain power to deal with the problems on a case-to-case basis if the administrative process is to be effective.

SEC v. Chenery, 332 U.S. 194, 202-03 (1947). Thus, an agency's discretion is "at its peak" when it decides "whether to address an issue by rulemaking or adjudication." *Am. Gas Ass'n v. FERC*, 912 F.2d 1496, 1519 (D.C. Cir. 1990). Proceeding by adjudication rather than rulemaking is especially appropriate "where important factors may vary radically from case to case." *Id.* The Supreme Court has approved of the FTC's case-by-case approach when using its "unfairness" authority under Section 5. *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 384-85 (1965) ("The proscriptions [of unfair or deceptive acts and

practices] in Section 5 are flexible, to be defined with particularity by the myriad of cases from the field of business, which necessarily give[] the Commission an influential role in interpreting Section 5 and in *applying it to the facts of particular cases arising out of unprecedented situations*." (emphasis added)); *see also Wyndham,* Slip Op. 18-25.[11]

As the Supreme Court has recognized, "[b]roadly worded constitutional and statutory provisions necessarily have been given concrete meaning and application by a process of case-by-case . . . decision." *NW Airlines v. Transp. Workers Union of Am.*, 451 U.S. 77, 95 (1981). The three-part statutory standard governing whether an act or practice is unfair is sufficient to give fair notice of what conduct is prohibited. *See* 15 U.S.C. § 45(n). Congress envisioned that the FTC would "develop[] and refin[e] its unfair practice criteria on a progressive, incremental basis." *Am. Fin. Servs.*, 767 F.2d at 979. The FTC is acting as Congress envisioned it would, and is in no way

[11] Indeed, in the field of data security, the FTC "has been involved in addressing online privacy issues for almost as long as there has been an online marketplace," and it has "repeatedly and consistently affirmed its authority to challenge unreasonable data security measures as 'unfair … acts or practices.'" Comm'n MTD Denial at 7. Thus, even though the FTC has not promulgated regulations governing data security, all companies holding electronic data have long been on notice that their security practices could be subject to FTC scrutiny. Contrary to LabMD's inaccurate assertion, the FTC has never "t[old] Congress that it lacks statutory authority" over data security. Pl.'s PI Mem. at 16; *see* Comm'n MTD Denial at 7-8.

violating LabMD's due process rights by adjudicating whether certain data security practices are unfair under Section 5 on a case-by-case basis.[12]

3. The FTC is not employing an unconstitutionally vague standard

The FTC's position – that failure to maintain reasonable data security measures can constitute an unfair act or practice within the meaning of Section 5 – does not establish an unconstitutionally vague behavioral standard. *See* N.D. Ga. Compl. ¶ 129-134. LabMD's main complaint is that what constitutes a reasonable data security program varies under the circumstances. The test for whether an economic regulation is unconstitutionally vague is undemanding, especially where, as here, plaintiff has the "ability to clarify" the standard as part of "an administrative process" prior to the imposition of any civil penalties. *Trans Union Corp. v. FTC*, 245 F.3d 809, 817 (D.C. Cir. 2001). Indeed, "[t]he Supreme Court has warned against the mechanical application of vagueness doctrine, emphasizing that an 'economic regulation is subject to a less strict vagueness test' and there should be 'greater tolerance of enactments with civil rather than criminal penalties because the consequences of imprecision are qualitatively less severe.'" *Harris v. Mexican Specialty Foods, Inc.*, 564 F.3d 1301, 1310-11

[12] Nor is the FTC required to "link its data-security standards" to HIPAA and HITECH. *See* N.D. Ga. Compl ¶ 134. As discussed *supra*, Part II.A, regulated entities commonly are regulated by more than one federal agency or statutory scheme.

(11th Cir. 2009) (quoting *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498–99 (1982)).

Agencies may use broad terms to describe permissible and impermissible conduct without running afoul of the void-for-vagueness doctrine:

> [When an agency establishes a standard that employs] the use of the terms like "adequate," "appropriate," [or] "suitable" . . . it is not impermissibly vague because "a reasonably prudent person, familiar with the conditions the regulations are meant to address and the objectives the regulations are meant to achieve, would have fair warning of what the regulations require." Courts recognize that "specific regulations cannot begin to cover all of the infinite variety of conditions which [regulated parties] must face," and that "by requiring [standards] to be too specific courts would be opening up large loopholes allowing conduct which should be regulated to escape regulation." Indeed, here, the [agency] was tasked with developing [standards] that apply to a diverse industry and the [agency] has explained that using qualifying terms like "adequate" is necessary to address the variety of conditions that exist at different companies.

Alliance for Natural Health U.S. v. Sebelius, 775 F. Supp. 2d 114, 132 (D.D.C. 2011) (quotation omitted). Like the regulation at issue in *Alliance*, specific regulations cannot begin to cover all of the infinite variety of conditions which companies face with respect to data security.

D. Plaintiff does not make a valid "structural due process" claim

Plaintiff's fourth claim for relief seeks to block the FTC's adjudicatory process for what it terms "facial and structural due process violations." N.D.

Ga. Compl. ¶137. This set of untenable arguments must be dismissed for failure to state a claim.

1. The FTC's structure and Rules of Practice do not violate due process

Plaintiff's main "structural due process" claim is that FTC Rules of Practice directing that motions to dismiss administrative complaints be resolved by the Commission itself "transgress constitutional limits on blending of prosecutorial, legislative, and adjudicative functions" in violation of plaintiff's due process rights. *Id.* ¶140. That contention is flatly wrong. *See FTC v. Cement Inst.*, 333 U.S. 683, 702-703 (1948); *Humphrey's Executor v. United States*, 295 U.S. 602, (1935) (finding FTC's exercise of both enforcement authority and quasi-adjudicatory functions constitutional). Due process "is not a technical conception with a fixed content unrelated to time, place and circumstances," *Cafeteria Workers v. McElroy*, 367 U.S. 886, 895 (1961), but "calls for such procedural protections as the particular situation demands." *Morrissey v. Brewer*, 408 U.S. 471, 481 (1972). In the context of administrative adjudications, courts long ago "reject[ed] the idea that the combination [of] judging [and] investigating functions is a denial of due process." *Withrow v. Larkin*, 421 U.S. 35, 52 (1975); *see also Intercontinental Indus., Inc. v. Am. Stock Exch.*, 452 F.2d 935, 943 (5th Cir. 1971) ("The principle is well established . . . that due process is not violated when an administrative agency exercises both investigative and judicial functions."). Rather, in formal agency adjudicatory proceedings, due process is satisfied

when the agency follows the requirements of the APA. *Withrow*, 421 U.S. 35 at 51-52; *see also FTC v. Cinderella Career & Finishing Schs, Inc.*, 404 F.2d 1308, 1315 (D.C. Cir. 1968) (citing numerous cases).

FTC Rule 3.22(a) accords plaintiff due process because it comports fully with the APA. The regulation provides that motions to dismiss administrative complaints "shall be directly referred to and ruled on by the Commission." 16 C.F.R. § 3.22(a).[13] Contrary to plaintiff's contention that only an administrative law judge may lawfully address a threshold motion, the APA contains no requirement that the ALJ play any role at all in adjudications conducted pursuant to 5 U.S.C. §§ 554 and 556, and it certainly does not require that ALJs address dispositive motions in the first instance. Indeed, the APA allows the *entire* adjudication to be presided over *either* by an ALJ, *or* by "the agency" *or* by "one or more members of the body which comprises the agency." 5 U.S.C. § 556(b).[14] The APA thus *a fortiori* permits the Commission to rule on a motion.

---

[13] The FTC amended Rule 3.22(b) in 2009. 16 C.F.R. Parts 3 & 4, Interim Final Rule, 74 Fed. Reg. 1804, 1809-1810 (Jan. 13, 2009). Previously, that Rule allowed the ALJ to resolve motions to dismiss in the first instance, 16 C.F.R. § 3.22 (2008), with subsequent review by the Commission, which could "adopt, modify, or set aside" the ALJ's decision, 16 C.F.R. § 3.44(a) (2008).

[14] Due process concerns regarding separation of prosecutorial and decisionmaking functions are accommodated by the APA's requirements that staff employees "engaged in the performance of investigative or prosecuting functions … may not … participate or advise in the decision … or agency review" and other protective provisions in 5 U.S.C. § 554(d); *see* 16 C.F.R. § 4.7(b). *See also Withrow*, 421 U.S. at 52. Of course, parties are also entitled to judicial review of a final agency decision. 5 U.S.C. § 702.

Moreover, the APA authorizes "[t]he agency . . . in its sound discretion, to issue a declaratory order to . . . remove uncertainty." 5 U.S.C. § 554(e). By using the term "the agency," the statute contemplates issuance of such an order by the agency acting as a whole and says nothing about an ALJ considering such rulings in the first instance. The Commission's order denying LabMD's Motion to Dismiss "removed uncertainty" about the scope of the FTC's authority over LabMD's data security practices. The ruling enabled the ALJ to narrow discovery and avoided wasteful development of irrelevant evidence.

Finally, both the APA and the FTC Act authorize the agency to review an ALJ's factual and legal conclusions de novo. 5 U.S.C. § 557(b); 15 U.S.C. § 45(b) & (c).[15] Because the APA allows the Commission to set aside an ALJ ruling, plaintiff's argument that due process requires giving an ALJ the first crack at dispositive legal issues makes no sense.

Even if plaintiff had stated a due process claim that theoretically could be viable, it would still fail in the present circumstances. "In order to make out a case of denial of procedural due process, there must be a showing of substantial prejudice." *Arthur Murray Studio of Wash., Inc. v. FTC*, 458 F.2d 622, 624 (5th Cir. 1972). Yet the complaint fails to allege any prejudice at all,

---

[15] The "highly deferential" standard on judicial review "is not altered merely because the [agency] disagrees with the ALJ, and [courts] defer to the inferences that the [agency] derives from the evidence, not to those of the ALJ." *Varnadore v. Sec'y of Labor*, 141 F.3d 625, 630 (6th Cir. 1998) (citations omitted); *see also Universal Camera Corp. v. NLRB*, 340 U.S. 474, 494 (1951).

let alone substantial prejudice, from the Commission's consideration of the motion to dismiss. And because the Commission would have reviewed de novo any ALJ decision dismissing or declining to dismiss the complaint, it is difficult to see how plaintiff possibly could have been prejudiced by the Commission's making that decision in the first instance.

2. Plaintiff has no valid ex post facto claim

As discussed above, 15 U.S.C. § 45(n) provides plaintiff with adequate notice of what the law requires. But even if it did not, plaintiff's claim that the FTC is unconstitutionally engaging in ex post facto enforcement of a law must be dismissed. *See* N.D. Ga. Compl. ¶ 141. The Supreme Court long ago established that the Constitution's prohibition on ex post facto law enforcement applies only to laws that are criminal or penal in nature. *See, e.g.*, *Carpenter v. Com. of Penn.*, 58 U.S. 456, 457 (1854). Even if the FTC issues a final cease and desist order, LabMD could incur sanctions only if the company takes further action that violate the order. Such a sanction is patently not criminal or penal in nature. *See, e.g.*, *Houston v. Williams*, 547 F.3d 1357, 1364 (11th Cir. 2008) (city's denial of certain services to sex offenders not penal in nature and, therefore, no subject to prohibition on ex post facto enforcement); *Dufrense v. Baer*, 744 F.2d 1543, 1550 (11th Cir. 1984) (amendments to the Sentencing Guidelines do not implicate ex post facto considerations "because the guidelines. . . are not criminal laws").

E. Plaintiff's First Amendment claims must be dismissed under Rule 12(b)(6)

LabMD has failed to nudge its First Amendment claims, *see* Fifth Claim for Relief, N.D. Ga. Compl. ¶¶144-150, "across the line from conceivable to plausible." *Twombly*, 550 U.S. at 570. The Court cannot plausibly infer a nexus between Mr. Daugherty's First Amendment activity – *i.e.*, his public criticism of the FTC in his published book and in other public statements – and the FTC actions LabMD challenges in this lawsuit.

Even assuming *arguendo* that Mr. Daugherty's expression constitutes protected speech, LabMD fails to satisfy any of the other established prerequisites for proving that the agency's enforcement action violated LabMD's First Amendment rights. LabMD cannot show that the FTC conduct at issue "adversely affected the protected speech," or that "there is a causal connection between the [FTC's purportedly] retaliatory actions and the adverse effect on speech." *Moton v. Cowart*, 631 F.3d 1337, 1341 (11th Cir. 2011) (quotation omitted). First, nothing in the administrative complaint itself challenges anything LabMD or Mr. Daugherty said or expressed, and the remedy proposed as part of that complaint would not restrict their expression in the future. And LabMD's factual contention that the enforcement action had a "chilling" effect on protected speech is utterly implausible, given that LabMD and Mr. Daugherty have not changed their public criticism of the FTC at all.

Moreover, LabMD cannot plausibly show that the FTC's investigation and enforcement action were brought to retaliate for LabMD's or Mr. Daugherty's criticism of the agency. That criticism began *after* the investigation was well underway; indeed, the entire premise of their public critique is that the agency's investigation of LabMD was itself unfair or improper. Just because the target of an agency investigation or enforcement action complains publicly about the agency's conduct cannot render any subsequent pursuit of the action unconstitutional. Otherwise, *any* target of an agency investigation could evade the agency's charges by publicly complaining about them.

LabMD's insinuation that Mr. Daugherty's publication of the book occurred at roughly the same time as the commencement of the enforcement action does not withstand even the minimal scrutiny Rule 12(b)(6) provides. Mr. Daugherty's book was published approximately three years *after* the FTC had begun investigating LabMD. *See* N.D. Ga. Compl. ¶ 26; Admin Compl. at 12. Courts have declined to infer retaliation unless the timing is "unusually suggestive." *Lauren v. DeFlaminis*, 480 F.3d 259, 267 (3d Cir. 2007)); *see also Swanson v. General Services Admin.*, 110 F.3d 1180, 1188 (5th Cir. 1997) (timing must be "close" to support inference of retaliation). A causal connection cannot plausibly be inferred from timing when the allegedly protected speech occurs in the *middle* of an ongoing action. *See Slattery v. Swiss Reinsurance Am. Corp.*, 248 F.3d 87, 95 (2d Cir. 2001) ("[Where] gradual adverse job actions began well before the plaintiff had ever engaged

in any protected [First Amendment] activity, an inference of retaliation does not arise.").

In essence, LabMD asks this Court to determine that the FTC selectively enforced its data security rules against the company because of its president's protected speech. But the "standard [for showing improper selective enforcement] is "demanding," and agency officials are entitled to a presumption "that they have properly discharged their official duties." *United States v. Armstrong*, 517 U.S. 456, 463-64 (1996). LabMD's allegations do not meet this exacting standard.[16] The FTC has brought numerous enforcement actions against firms across the country alleging unfair acts or practices in connection with data security; the action against LabMD – and the relief related to data security sought by the proposed order – was not novel. LabMD has not come close to showing abuse of the FTC's "significant discretion, analogous to that of a criminal prosecutor, in choosing their targets in administrative enforcement proceedings." *Arnold v. CFTC*,

[16] There is nothing constitutionally improper about the subpoena issued to the President and CEO of LabMD regarding statements he made in a book relating to the very subject matter of the administrative proceeding. N.D. Ga. Compl. ¶ 53. Indeed, the ALJ denied enforcement of the subpoena on the ground that the information sought was not relevant, not that it intruded on Mr. Daugherty's speech rights. *See In re LabMD, Inc.*, FTC Docket No. 9357, ALJ Order on Respondent's Motion for a Protective Order at 8 (Nov. 22, 2013) (FTC Ex. 7). Even if the subpoena were somehow constitutionally improper, which it was not, it was issued not by the Commission but by its separated complaint counsel. Complaint counsel's actions and statements as an advocate in an administrative adjudication cannot be attributed to the Commission as a whole.

987 F. Supp. 1463, 1468 (S.D. Fla. 1997) (citing *Butz v. Economou*, 438 U.S. 478, 515 (1978)).

III. LabMD's motion for a preliminary injunction must be denied

"A preliminary injunction is an extraordinary and drastic remedy" *ACLU of Fla., Inc. v. Miami–Dade Cnty. Sch. Bd.*, 557 F.3d 1177, 1198 (11th Cir. 2009), and is "not to be granted unless the movant clearly [satisfies] the burden of persuasion as to all four" of the following factors: (1) a substantial likelihood of success on the merits; (2) irreparable injury in the absence of injunction; (3) the threatened injury to the movant outweighs whatever damage the proposed injunction may cause the opposing party; and (4) that the injunction would not be adverse to the public interest. *Siegel v. LePore*, 234 F.3d 1163, 1176 (11th Cir. 2000) (en banc); *see also All Care Nursing Serv., Inc. v. Bethesda Mem'l Hosp., Inc.*, 887 F.2d 1535, 1537 (11th Cir. 1989) (a showing on all four factors is required). On the first factor, the Supreme Court has made clear that "[i]t is not enough that the chance of success on the merits be 'better than negligible;'" rather, the party seeking a preliminary injunction—or a stay of an administrative agency proceeding—must make a "strong showing that [it] is likely to succeed on the merits," and "more than a mere 'possibility' of relief is required." *Nken v. Holder*, 556 U.S. 418, 434 (2009). The likelihood of success on the merits is generally considered the most important of the four factors. *See Garcia–Mir v. Meese*, 781 F.2d 1450, 1453 (11th Cir. 1986). As shown above, this Court lacks jurisdiction and thus cannot even reach plaintiff's claims. Nor can LabMD succeed on the merits

because its claims are not viable. That is fatal to LabMD's motion and the Court need not proceed further. "If the movant fails to establish one or more of the four prerequisites, the Court is not required to address the others." *Kramer v. Conway*, 962 F. Supp. 2d 1333, 1343 (N.D. Ga. 2013) (Duffey, J.) (citing *Church v. City of Huntsville*, 30 F.3d 1332, 1342 (11th Cir. 1994)).

Nonetheless, it bears noting that LabMD also fails to meet the other three preliminary injunction factors. *See Nken*, 556 U.S. at 434-35 ("simply showing some 'possibility of irreparable injury' fails to satisfy the second factor"). The Supreme Court has made clear that the type of hardship LabMD will experience by awaiting the FTC's decision – "litigation expense, even substantial and unrecoupable cost" – "does not constitute irreparable injury." *Standard Oil* at 244 (quotation omitted). Moreover, LabMD has not explained how the alleged lapse of its insurance policy on May 6 creates an irreparable injury or an exigent circumstance. According to its own exhibits, LabMD knew that insurers were becoming reluctant to renew LabMD's policies no later than mid-January 2014. *See* N.D. Ga. Compl. Ex. 2. Even earlier, on January 6, 2014, LabMD's CEO sent a letter to the staff and other interested parties, announcing that the company would be closed effective January 15, 2014. *See* N.D. Ga. Compl. Ex. 3. In those circumstances, LabMD cannot show any harm stemming from the May 6 lapse in an insurance policy, especially since LabMD had a case pending before the district court in D.C. in January 2014. Yet LabMD did not ask that court for a preliminary injunction or plead exigency; instead, it dismissed its case

voluntarily – and then waited more than a month to file the present case. That is not the action of a company that truly faces the prospect of irreparable harm. To the degree that it will suffer any harm on May 6, LabMD is the sole cause of its purported hardships.

Additionally, LabMD will not suffer any harm to its First Amendment rights. Its president may continue to engage in speech critical of the FTC, as he has for many years. Indeed, the complaint does not allege any way in which his speech (or that of LabMD itself) has been chilled. *See, e.g.*, *Blum v. Bankatlantic Fin. Corp.*, 925 F.2d 1357, 1363 (11th Cir. 1991) (irreparable harm must be "concrete"). Accordingly, the second factor required for preliminary injunctive relief is unmet.

In contrast to the absence of cognizable harm to LabMD, the FTC and the public will suffer harm if the Court were to grant a preliminary injunction. As *Ewing* and related cases make clear, agencies and the public have a strong interest in an orderly administrative process, unencumbered by premature involvement by the federal judiciary. The public interest would be poorly served by hobbling the proper administrative function of a federal agency that is tasked with protecting consumers from unfair and deceptive trade practices. *See* 15 U.S.C. § 45. That is particularly the case here, where thousands of people have allegedly suffered potentially severe harm as a result of unauthorized disclosure of LabMD's data, and many more could be exposed by further unauthorized disclosures.

In short, all of plaintiff's arguments for why an injunction would be equitable and in the public interest depend on its argument that the FTC has exceeded its legal authority. *See* Pl's Mot. Prelim. Injunction at 29. Because it cannot succeed on the merits of this claim, plaintiff also cannot show that an injunction would be equitable or in the public interest.

CONCLUSION

For the foregoing reasons, plaintiff's complaint must be dismissed and its motion for a preliminary injunction must be denied.

Dated: April 7, 2014

Respectfully submitted,

Of counsel:
JONATHAN E. NUECHTERLEIN
General Counsel
JOHN F. DALY
Deputy General Counsel for Litigation

JOEL MARCUS-KURN
Attorney

Office of General Counsel
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

STUART F. DELERY
Assistant Attorney General

MAAME EWUSI-MENSAH FRIMPONG
Deputy Assistant Attorney General

MICHAEL S. BLUME
Director

/s/ Adrienne E. Fowler
ADRIENNE E. FOWLER
LAUREN E. FASCETT
Trial Attorneys

U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street, N.W.
Washington, D.C. 20530
Tel: 202-616-3466
Adrienne.E.Fowler@usdoj.gov
Lauren.Fascett@usdoj.gov

CERTIFICATE OF COMPLIANCE

I certify that the documents to which this certificate is attached have been prepared with one of the font and point selections approved by the Court in LR 5.1B for documents prepared by computer – namely Century Schoolbook, 13 pt.

Dated: April 7, 2014

/s/ Adrienne E. Fowler
ADRIENNE E. FOWLER
LAUREN E. FASCETT
Trial Attorneys

U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street, N.W.
Washington, D.C. 20530
Tel: 202-616-3466
Adrienne.E.Fowler@usdoj.gov
Lauren.Fascett@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on April 7, 2014, I caused a true and correct copy of the foregoing via CM/ECF on:

Ronald L. Raider
Burleigh L. Singleton
William D. Meyer
KILPATRICK TOWNSEND & STOCKTON LLP
1100 Peachtree Street, NE, Suite 2800
Atlanta, Georgia 30309

Michael D. Pepson
CAUSE OF ACTION
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006

Furthermore, the following was provided with a copy via overnight delivery:

Reed D. Rubinstein
DINSMORE & SHOHL, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004

Dated: April 7, 2014

/s/ Adrienne E. Fowler
ADRIENNE E. FOWLER
LAUREN E. FASCETT
Trial Attorneys

U.S. Department of Justice
Civil Division
Consumer Protection Branch
450 5th Street, N.W.
Washington, D.C. 20530
Tel: 202-616-3466
Adrienne.E.Fowler@usdoj.gov
Lauren.Fascett@usdoj.gov

PRIVACY ONLINE: A REPORT TO CONGRESS

FEDERAL TRADE COMMISSION

JUNE 1998

FEDERAL TRADE COMMISSION

Robert Pitofsky	Chairman
Mary L. Azcuenaga	Commissioner
Sheila F. Anthony	Commissioner
Mozelle W. Thompson	Commissioner
Orson Swindle	Commissioner

BUREAU OF CONSUMER PROTECTION

Authors

Martha K. Landesberg	Division of Credit Practices
Toby Milgrom Levin	Division of Advertising Practices
Caroline G. Curtin	Division of Advertising Practices
Ori Lev	Division of Credit Practices

Survey Advisors

Manoj Hastak	Division of Advertising Practices
Louis Silversin	Bureau of Economics
Don M. Blumenthal	Litigation and Customer Support Center Information and Technology Management Office
George A. Pascoe	Litigation and Customer Support Center Information and Technology Management Office

TABLE OF CONTENTS

Executive Summary i

I. Introduction 1

II. History and Overview 2
A. The Federal Trade Commission's Approach to Online Privacy 2
B. Consumer Privacy Online 2
1. Growth of the Online Market 2
2. Privacy Concerns 3
C. Children's Privacy Online 4
1. Growth in the Number of Children Online 4
2. Safety and Privacy Concerns 4

III. Fair Information Practice Principles 7
A. Fair Information Practice Principles Generally 7
1. Notice/Awareness 7
2. Choice/Consent 8
3. Access/Participation 9
4. Integrity/Security 10
5. Enforcement/Redress 10
B. Application of Fair Information Practice Principles to Information Collected From Children 12
1. Parental Notice/Awareness and Parental Choice/Consent 12
2. Access/Participation and Integrity/Security 13

IV. Industry Association Guidelines 15
A. Industry Association Guidelines 15
1. Notice/Awareness 15
2. Choice/Consent 16
3. Access/Participation 16
4. Integrity/Security 16
5. Enforcement/Redress 16
B. Guidelines Regarding Children's Information 17

V. Survey of Commercial Web Sites 19
A. Overview 19
B. General Survey Findings 21
1. Web Sites 21
2. Personal Information Collection 22
3. Frequency of Disclosures 27
4. Nature of Disclosures 29
C. Children's Survey Findings 31

1. Personal Information Collection from Children 31
2. Frequency of Disclosures 34
3. Nature of Disclosures 35
4. Parental Involvement 37

VI. Conclusions 39

Endnotes 45

Appendix A: Methodology

Appendix B: Surfer Instructions (General and Children's Surveys)

Appendix C: Survey Samples and Results

Appendix D: Supporting Data Tables

Appendix E: Industry Guidelines

EXECUTIVE SUMMARY

- A medical clinic's online doctor-referral service invites consumers to submit their name, postal address, e-mail address, insurance company, any comments concerning their medical problems, and to indicate whether they wish to receive information on any of a number of topics, including urinary incontinence, hypertension, cholesterol, prostate cancer, and diabetes. The online application for the clinic's health education membership program asks consumers to submit their name, address, telephone number, date of birth, marital status, gender, insurance company, and the date and location of their last hospitalization. The clinic's Web site says nothing about how the information consumers provide will be used or whether it will be made available to third parties.

- A child-directed site collects personal information, such as a child's full name, postal address, e-mail address, gender, and age. The site also asks a child whether he or she has received gifts in the form of stocks, cash, savings bonds, mutual funds, or certificates of deposit; who has given these gifts; whether monetary gifts were invested in mutual funds, stocks, or bonds; and whether the child's parents own mutual funds. Elsewhere on the site, contest winners' full name, age, city, state and zip code are posted. The Web site does not tell children to ask their parents for permission before providing personal information and does not appear to take any steps to involve parents. Further, the site says nothing about whether the information is disclosed to third parties.

* * *

The World Wide Web is an exciting new marketplace for consumers. It offers easy access to a broad array of goods, services, and information, but also serves as a source of vast amounts of personal information about consumers, including children. While the online consumer market is growing exponentially, there are also indications that consumers are wary of participating in it because of concerns about how their personal information is used. As the above examples show, these concerns are real, for both adults and children.

The Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace and has held a series of workshops and hearings on such issues. Throughout, the Commission's goal has been to encourage and facilitate effective self-

regulation as the preferred approach to protecting consumer privacy online. These efforts have been based on the belief that greater protection of personal privacy on the Web will not only protect consumers, but also increase consumer confidence and ultimately their participation in the online marketplace. In this report, the Commission summarizes widely-accepted principles regarding information collection, use, and dissemination; describes the current state of information collection and privacy protection online; and assesses the extent of industry's self-regulatory response.

Government studies in the United States and abroad have recognized certain core principles of fair information practice. These principles are widely accepted as essential to ensuring that the collection, use, and dissemination of personal information are conducted fairly and in a manner consistent with consumer privacy interests. These core principles require that consumers be given *notice* of an entity's information practices; that consumers be given *choice* with respect to the use and dissemination of information collected from or about them; that consumers be given *access* to information about them collected and stored by an entity; and that the data collector take appropriate steps to ensure the *security* and integrity of any information collected. Moreover, it is widely recognized that fair information practice codes or guidelines should contain enforcement mechanisms to ensure compliance with these core principles. With respect to the collection of information from children, a wide variety of public policies recognize the important supervisory role of parents in commercial transactions involving their children. Parental control is also the touchstone for application of fair information practice policies to the collection of information from children.

The Commission solicited industry association fair information practice guidelines to assess their conformity with these core principles. This assessment shows that industry association guidelines generally encourage members to provide notice of their information practices and some choice with respect thereto, but fail to provide for access and security or for enforcement mechanisms.

The Commission also examined the practices of commercial sites on the World Wide Web. The Commission's survey of over 1,400 Web sites reveals that industry's efforts to encourage

voluntary adoption of the most basic fair information practice principle — notice — have fallen far short of what is needed to protect consumers. The Commission's survey shows that the vast majority of Web sites — upward of 85% — collect personal information from consumers. Few of the sites — only 14% in the Commission's random sample of commercial Web sites — provide any notice with respect to their information practices, and fewer still — approximately 2% — provide notice by means of a comprehensive privacy policy. The results with respect to the collection of information from children are also troubling. Eighty-nine percent of children's sites surveyed collect personal information *from children*. While 54% of children's sites provide some form of disclosure of their information practices, few sites take any steps to provide for meaningful parental involvement in the process. Only 23% of sites even tell children to seek parental permission before providing personal information, fewer still (7%) say they will notify parents of their information practices, and less than 10% provide for parental control over the collection and/or use of information from children. The Commission's examination of industry guidelines and actual online practices reveals that effective industry self-regulation with respect to the online collection, use, and dissemination of personal information has not yet taken hold.

In light of the Commission's findings and significant consumer concerns regarding privacy online, it is evident that substantially greater incentives are needed to spur self-regulation and ensure widespread implementation of basic privacy principles. The Commission is currently considering such incentives and possible courses of action to adequately protect the privacy of online consumers generally. The Commission will make its recommendations on this subject this summer.

In the specific area of children's online privacy, however, the Commission now recommends that Congress develop legislation placing parents in control of the online collection and use of personal information from their children. Such legislation would require Web sites that collect personal identifying information from children to provide actual notice to parents and obtain parental consent. The timing of such notice and consent would vary depending on the age of the child, and the nature and uses of the information collected. Such legislation would protect children and ensure that parents have knowledge of, and control over, the collection of

information from their children.

The development of the online marketplace is at a critical juncture. If growing consumer concerns about online privacy are not addressed, electronic commerce will not reach its full potential. To date, industry has had only limited success in implementing fair information practices and adopting self-regulatory regimes with respect to the online collection, use, and dissemination of personal information. Accordingly, the Commission now recommends legislation to protect children online and this summer will recommend an appropriate response to protect the privacy of all online consumers.

I. INTRODUCTION

This report to Congress provides an assessment of the effectiveness of self-regulation as a means of protecting consumer privacy on the World Wide Web ("the Web").[1] It is based on a comprehensive online survey of the information practices of commercial Web sites, including sites directed to children, conducted in March 1998; an examination of current industry guidelines governing information practices online; and the record developed in Commission hearings and workshops held since 1995.

Part II of the report provides a brief history of the Commission's work in the area of online privacy, and a summary of the privacy concerns raised by the new online marketplace. Part III describes what have come to be recognized as the core principles of privacy-protective information practices. Part IV then compares current industry guidelines with these generally accepted principles, and Part V presents the findings of the Commission's survey of Web sites. Part VI sets forth the Commission's conclusions.

II. HISTORY AND OVERVIEW

A. THE FEDERAL TRADE COMMISSION'S APPROACH TO ONLINE PRIVACY

The Commission has been involved in addressing online privacy issues for almost as long as there has been an online marketplace. In April 1995, staff held its first public workshop on privacy on the Internet, and in November of that year the Commission held hearings on online privacy as part of its extensive hearings on the implications of globalization and technological innovation for competition and consumer protection issues.

In June 1996, the Commission conducted a two-day workshop to explore privacy concerns raised by the online collection of personal information, and the special concerns raised by the collection of personal information from children. The workshop considered an array of alternatives to address those concerns, including industry self-regulation, technology-based solutions, consumer and business education, and government regulation. A summary of the workshop testimony was published by the Commission in a December 1996 staff report entitled *Consumer Privacy on the Global Information Infrastructure*. A second workshop in June 1997 delved more deeply into these issues.[2] In all of these endeavors the Commission's goals have been (1) to identify potential consumer protection issues related to online marketing and commercial transactions; (2) to provide a public forum for the exchange of ideas and presentation of research and technology; and (3) to encourage effective self-regulation.[3]

B. CONSUMER PRIVACY ONLINE

1. GROWTH OF THE ONLINE MARKET

The World Wide Web is an exciting new marketplace for consumers. It offers easy access not only to a vast array of goods and services, but also to rich sources of information that enable

consumers to make better-informed purchasing decisions. It also offers the convenience of shopping from the office or home. This information-rich medium also serves as a source of vast amounts of personal information about consumers. Commercial Web sites collect personal information explicitly through a variety of means, including registration pages, user surveys, and online contests, application forms, and order forms. Web sites also collect personal information through means that are not obvious to consumers, such as "cookies."[4]

The online consumer market is growing exponentially. In early 1997, 51 million adults were already online in the U.S. and Canada,[5] and 73% reported that they had shopped for product information on the World Wide Web.[6] By December 1997, the number of adults online in the U.S. and Canada had climbed to 58 million, and 10 million had actually purchased a product or service online.[7] Analysts estimate that Internet advertising — which totaled approximately $301 million in 1996 — will swell to $4.35 billion by the year 2000.[8]

2. PRIVACY CONCERNS

While these figures suggest that the online marketplace is growing rapidly, there are also indications that consumers are wary of participating in it. Surveys have shown that increasing numbers of consumers are concerned about how their personal information is used in the electronic marketplace. This research indicates that consumers have less confidence in how online service providers and merchants handle personal information than they have in how traditionally offline institutions, such as hospitals and banks, handle such information.[9] In fact, a substantial number of online consumers would rather forego information or products available through the Web than provide a Web site personal information without knowing what the site's information practices are.[10] According to the results of a March 1998 *Business Week* survey, consumers not currently using the Internet ranked concerns about the privacy of their personal information and communications as the top reason they have stayed off the Internet.[11] Clearly, consumers care deeply about the privacy and security of their personal information in the online environment and are looking for greater protections.[12] These findings suggest that consumers will continue to distrust online companies and will remain wary of engaging in electronic commerce until

meaningful and effective consumer privacy protections are implemented in the online marketplace. If such protections are not implemented, the online marketplace will fail to reach its full potential.

C. CHILDREN'S PRIVACY ONLINE

1. GROWTH IN THE NUMBER OF CHILDREN ONLINE

Children represent a large and rapidly growing segment of online consumers and are being actively targeted by commercial Web sites.[13] Children use the Web for a wide variety of activities, including homework, informal learning, browsing, playing games, corresponding with electronic pen pals by e-mail, placing messages on electronic bulletin boards and participating in chat rooms.[14] Among the activities most attractive to children are those that allow them to communicate directly with their peers, for example, chat rooms, bulletin boards and e-mail.[15] Almost 10 million (14%) of America's 69 million children are now online, with over 4 million accessing the Internet from school and 5.7 million from home.[16] Children are also avid consumers and represent a large and powerful segment of the marketplace. They are estimated to spend billions of dollars a year, and to influence the expenditure of billions more.[17] Their growing presence online, therefore, creates enormous opportunities for marketers to promote their products and services to an eager audience.[18] At the same time, the Web offers an easy way to collect large amounts of detailed marketing data from and about children.

2. SAFETY AND PRIVACY CONCERNS

A wide variety of detailed personal information is being collected online from and about children, often without actual notice to or an opportunity for control by parents.[19] This information may be collected from children at various places on a site: when the child is registering for a contest, enrolling in an electronic pen pal program, completing a survey, or playing a game. A child may also reveal such personal information in the course of participating in chat rooms or posting messages on electronic bulletin boards — areas that are publicly accessible to anyone surfing the Web.[20] These practices present unique privacy and safety

concerns because of the particular vulnerability of children, the immediacy and ease with which information can be collected from them, and the ability of the online medium to circumvent the traditional gatekeeping role of the parent.

The most potentially serious safety concern is presented by the posting of personal identifying information by and about children — *i.e.*, information that can be used to identify children, such as name, postal or e-mail address — in interactive public areas, like chat rooms and bulletin boards, that are accessible to all online users. These activities enable children to communicate freely with strangers, including adults. The FBI and Justice Department's "Innocent Images" investigation has revealed that online services and bulletin boards are quickly becoming the most powerful resources used by predators to identify and contact children.[21] Further, anecdotal evidence indicates that many children surfing the Web claim to have experienced problems such as attempted password theft and inappropriate advances by adults in children's chat rooms.[22]

Traditionally, parents have instructed children to avoid speaking with strangers. The collecting or posting of personal information in chat rooms and on bulletin boards online runs contrary to that traditional safety message. Children are told by parents not to talk to strangers whom they meet on the street, but they are given a contrary message by Web sites that encourage them to interact with strangers in their homes via the Web. The dangers in the Web environment are heightened by the fact that children cannot determine whether they are dealing with another child or an adult posing as a child.

In addition to these safety issues are privacy concerns raised by commercial Web sites' collection of personal information from children for marketing purposes. As described below, the practice is widespread and includes the collection of personal information from even very young children without any parental involvement or awareness.

There is considerable concern about online collection practices that bypass parents, who have traditionally protected children from marketing abuses.[23] Children generally lack the developmental capacity and judgment to give meaningful consent to the release of personal information to a third party.[24] This is an even greater problem when children are offered an

incentive for releasing personal information, or when release of personal information is a prerequisite to registering for a contest, joining a kid's club, or playing a game.[25]

Survey data confirm that parents strongly favor limiting the collection and use of personal information from and about their children. For example, 97% of parents whose children use the Internet believe Web sites should not sell or rent personal information relating to children, and 72% object to a Web site's requesting a child's name and address when the child registers at the site, even if such information is used only internally.[26]

In sum, the immediacy and ease with which personal information can be collected from children online, combined with the limited capacity of children to understand fully the potentially serious safety and privacy implications of providing that information, have created deep concerns about current information practices involving children online.

III. FAIR INFORMATION PRACTICE PRINCIPLES

A. FAIR INFORMATION PRACTICE PRINCIPLES GENERALLY

Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information — their "information practices" — and the safeguards required to assure those practices are fair and provide adequate privacy protection.[27] The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices.[28] Common to all of these documents [hereinafter referred to as "fair information practice codes"] are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

1. NOTICE/AWARENESS

The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.[29] Moreover, three of the other principles discussed below — choice/consent, access/participation, and enforcement/redress — are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.[30]

While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:

- identification of the entity collecting the data;[31]
- identification of the uses to which the data will be put;[32]
- identification of any potential recipients of the data;[33]

- the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);[34]
- whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information;[35] and
- the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.[36]

Some information practice codes state that the notice should also identify any available consumer rights, including: any choice respecting the use of the data;[37] whether the consumer has been given a right of access to the data;[38] the ability of the consumer to contest inaccuracies;[39] the availability of redress for violations of the practice code;[40] and how such rights can be exercised.[41]

In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web. To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site's home page and any Web page where information is collected from the consumer. It should also be unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge.

2. CHOICE/CONSENT

The second widely-accepted core principle of fair information practice is consumer choice or consent.[42] At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information — *i.e.*, uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information; opt-out regimes require affirmative steps to prevent the collection and/or use of such information. The distinction lies in the default rule when no affirmative steps are taken by the consumer.[43] Choice can also involve more than a binary yes/no option. Entities can, and do, allow consumers to tailor the nature of the information they reveal and the uses to which it will be put.[44] Thus, for example, consumers can be provided separate choices as to whether they wish to be on a company's general internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers to exercise their choice.

In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a Web site, thus effectively eliminating any need for default rules.[45]

3. ACCESS/PARTICIPATION

Access is the third core principle. It refers to an individual's ability both to access data about him or herself — *i.e.*, to view the data in an entity's files — and to contest that data's accuracy and completeness.[46] Both are essential to ensuring that data are accurate and complete. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.[47]

4. INTEGRITY/SECURITY

The fourth widely accepted principle is that data be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.[48]

Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.[49] Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.[50]

5. ENFORCEMENT/REDRESS

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them.[51] Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.[52]

a. Self-Regulation[53]

To be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress).[54] Mechanisms to ensure compliance include making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association;[55] external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue.[56] A self-regulatory regime with many of these principles has recently been adopted by the individual reference services industry.[57]

Appropriate means of individual redress include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed.[58] Thus, a self-regulatory system should provide a means to investigate complaints from individual consumers and ensure that consumers are aware of how to access such a system.[59]

If the self-regulatory code has been breached, consumers should have a remedy for the violation. Such a remedy can include both the righting of the wrong (*e.g.*, correction of any misinformation, cessation of unfair practices) and compensation for any harm suffered by the consumer.[60] Monetary sanctions would serve both to compensate the victim of unfair practices and as an incentive for industry compliance. Industry codes can provide for alternative dispute resolution mechanisms to provide appropriate compensation.

b. Private Remedies

A statutory scheme could create private rights of action for consumers harmed by an entity's unfair information practices. Several of the major information practice codes, including the seminal 1973 HEW Report, call for implementing legislation.[61] The creation of private remedies would help create strong incentives for entities to adopt and implement fair information practices and ensure compensation for individuals harmed by misuse of their personal information. Important questions would need to be addressed in such legislation, *e.g.*, the definition of unfair information practices; the availability of compensatory, liquidated and/or punitive damages;[62] and the elements of any such cause of action.

c. Government Enforcement

Finally, government enforcement of fair information practices, by means of civil or criminal penalties, is a third means of enforcement. Fair information practice codes have called for some government enforcement, leaving open the question of the scope and extent of such powers.[63] Whether enforcement is civil or criminal likely will depend on the nature of the data at issue and the violation committed.[64]

B. APPLICATION OF FAIR INFORMATION PRACTICE PRINCIPLES TO INFORMATION COLLECTED FROM CHILDREN

The fair information practice codes discussed above do not address personal information collected from children. They are, however, applicable to parents, in light of the special status that children generally have been accorded under the law. This status as a special, vulnerable group is premised on the belief that children lack the analytical abilities and judgment of adults.[65] It is evidenced by an array of federal and state laws that protect children, including those that ban sales of tobacco and alcohol to minors, prohibit child pornography, require parental consent for medical procedures, and make contracts with children voidable. In the specific arenas of marketing and privacy rights, moreover, several federal statutes and regulations recognize both the need for heightened protections for children and the special role that parents play in implementing these protections.[66]

1. PARENTAL NOTICE/AWARENESS AND PARENTAL CHOICE/CONSENT

It is *parents* who should receive the notice and have the means to control the collection and use of personal information from their children. The Commission staff set forth this principle in a July 15, 1997 letter to the Center for Media Education.[67] In addition, the letter identifies certain practices that appear to violate the Federal Trade Commission Act:

(a) It is a deceptive practice to represent that a site is collecting personal identifying information from a child for a particular purpose (*e.g.* to earn points to redeem a premium), when the information will also be used for another purpose that parents would find material, in the absence of a clear and prominent disclosure to that effect; and

(b) It is likely to be an unfair practice to collect personal identifying information, such as a name, e-mail address, home address, or phone number, from children and to sell or otherwise disclose such identifying information to third parties, or to post it publicly

online, without providing parents with adequate notice and an opportunity to control the collection and use of the information through prior parental consent.

This letter applies the Commission's Section 5 authority for the first time to the principles of notice and choice in the online collection of information from children. The principles set out in the staff opinion letter form an appropriate basis for public policy in this area.

To assure that notice and choice are effective, a Web site should provide *adequate notice* to a parent that the site wishes to collect personal identifying information from the child,[68] and give the parent an opportunity to control the collection and use of that information. Further, according to the staff opinion letter, in cases where the information may be released to third parties or the general public, the site should obtain the parent's *actual or verifiable consent*[69] to its collection.[70]

The content of the notice should include at a minimum, the elements described above,[71] but, in addition, should take into account the fact that online activities may be unique and unfamiliar to parents. Thus, a notice should be sufficiently detailed to tell parents clearly the type(s) of information the Web site collects from children and the steps parents can take to control the collection and use of their child's personal information. Where a Web site offers children interactive activities such as chat, message boards, free e-mail services, posting of home pages and key pal programs, it should explain to parents the nature of these activities and that children's participation enables others to communicate directly with them. Such notice empowers parents to monitor their children's interactions and to help protect their children from the risks of inappropriate online interactions.

2. ACCESS/PARTICIPATION AND INTEGRITY/SECURITY

Since parents may not be fully aware of what personal information a site has collected from their child, the access/participation principle is a particularly important one with respect to information collected from children. To provide informed consent to the retention and/or use of information collected from their children, parents need to be given access to the information collected from their children, particularly if any of the information is collected prior to providing notice to the parent. The principle of integrity, which addresses the accuracy of the data, is also

important for children's information. Parents have an interest in assuring that whatever information Web sites collect from children or have otherwise obtained about their children is accurate. This is particularly important in contexts that involve decisions that impact on the child or family, such as educational or health decisions. In addition, since children's information is considered to be a more sensitive type of information, sites should take the same steps identified above to assure that children's data is secure from unauthorized uses or disclosures.

IV. INDUSTRY ASSOCIATION GUIDELINES

Throughout the series of Commission workshops on online privacy issues, the online industry has asserted that self-regulation is a more efficient and effective means of creating online privacy protections than government regulation. To gauge the status and effectiveness of current self-regulatory efforts, on March 5, 1998 the Commission published a *Federal Register* Notice (the "Notice") requesting that trade associations and industry groups voluntarily submit copies of their online information practice guidelines and principles.[72] Nine industry-specific guidelines were submitted.[73] Copies of these guidelines are included in Appendix E. The guidelines do not address all of the core fair information practice principles discussed above, but all encourage companies to provide notice of at least some of their information practices, and most encourage choice with respect to the disclosure of personal information to third parties. For the most part, the submitted guidelines do not address access or security. Most importantly, very few provide any kind of enforcement mechanism, an essential element of effective self-regulation.

A. INDUSTRY ASSOCIATION GUIDELINES

1. NOTICE/AWARENESS

All of the guidelines submitted encourage member companies to provide at least some notice of their information practices. The extent of the suggested notice ranges from a general recommendation to post a privacy policy on Web sites,[74] to more specific exhortations to provide notice with respect to the nature of information collected, how it is collected, its intended uses, the nature and purposes of any intended disclosures to third parties, and the mechanism to opt-out of any third-party disclosure.[75] None of the guidelines discusses the need to provide notice about access or security.

2. CHOICE/CONSENT

Most of the guidelines suggest that member companies provide some degree of choice with respect to the use of personal information.[76] Here too there is a range in what is suggested by the guidelines. Some guidelines suggest giving consumers choice with respect to most secondary uses of their information, both external (*i.e.*, disclosure to third parties) and internal (*i.e.*, marketing back to the consumer);[77] others suggest giving consumers a choice solely with respect to external uses.[78] All of the guidelines speak of choice in terms of opt-out options for the consumer; none adopts an opt-in regime for adult consumers.

3. ACCESS/PARTICIPATION

Several of the industry guidelines address consumer access to information by providing generally that procedures should be established to ensure accuracy of the information, including allowing consumers access to, and the opportunity to correct, information collected about them.[79] Other guidelines fail to make any reference to the access principle.

4. INTEGRITY/SECURITY

Only the banking and financial industry association guidelines, and the individual reference services guidelines, make any reference to security issues. These guidelines call generally for appropriate security procedures, including the limitation of employee access to data.[80]

5. ENFORCEMENT/REDRESS

With limited exception,[81] the submitted guidelines contain no enforcement mechanisms. Only one of the guidelines conditions further membership and information sharing on adherence to the guidelines.[82] One other set of guidelines provides for peer review of alleged violations, but it is not binding.[83] All of the other guidelines and policies submitted are merely exhortatory.[84] As discussed above, the absence of enforcement mechanisms significantly weakens the effectiveness of industry-promulgated guidelines as a self-regulatory tool. This is especially true if member companies fail to voluntarily adhere to suggested policies.

B. GUIDELINES REGARDING CHILDREN'S INFORMATION

The Commission received two sets of guidelines regarding collection and use of information from children in response to its March 1998 Notice: the Children's Advertising Review Unit of the Council of Better Business Bureaus, Inc.'s ("CARU") *Guidelines for Interactive Electronic Media* ("*CARU Guidelines*") and the Direct Marketing Association's ("DMA") *Online Data Collection from or about Children* ("*DMA Children's Guidelines*").[85] Both guidelines address younger children.[86]

The *CARU Guidelines*, issued in April 1997, are consistent with the principles outlined in the staff opinion letter described above. They require that advertisers make "reasonable efforts" to provide notice and choice to parents when information is collected from children online, including the collection of information through "passive tracking."[87] In all cases, the notice must specify the means by which parents can correct or remove the information collected from a company's database.[88] The guidelines require prior parental consent (opt-in) to the collection of personal identifying information from children under the following circumstances: (1) when the information would enable the recipient to contact the child offline, regardless of the intended use; (2) when the information would be publicly posted so as to enable others to communicate directly with the child online; and (3) when the information would be shared with third parties.[89] Under other circumstances, such as the collection for internal use of an e-mail address, first name, or hometown, the site must provide notice to the parent and an opportunity to opt-out.[90] If a site collects only anonymous or aggregate information, the guidelines require notice of the intended uses of the information, but not parental consent.[91]

In addition, CARU has an enforcement mechanism in place to promote compliance with its online privacy guidelines,[92] and has achieved a remarkably high level of compliance under this mechanism in the offline media over a long period of time.[93] While CARU has worked to encourage Web sites to adhere to its privacy guidelines with respect to the collection of personal information from children online, to date it has not achieved the same widespread adherence it has achieved in other media.[94]

The *DMA Children's Guidelines*, which were adopted in January 1997, do not conform to the principles set forth in the staff opinion letter. The DMA is working now, however, to strengthen and refine its children's guidelines. The current *DMA Children's Guidelines* urge marketers to: (1) take into account a child's age, knowledge, sophistication, and maturity when collecting information; (2) encourage young children to obtain their parents' permission;[95] and (3) support parental control over the collection of data from children through notice and opt-out.[96] These guidelines do not call for *actual* notice to parents or for prior parental consent, even where the information is disclosed to third parties or otherwise made publicly available.

V. SURVEY OF COMMERCIAL WEB SITES

A. OVERVIEW

With these fair information practice principles and industry guidelines as background, the Commission conducted a survey of commercial sites on the World Wide Web. In July 1997, the Commission set out the objective of this survey: to determine whether self-regulation is an effective means of protecting consumer privacy on the Web. The Commission stated that it would measure the effectiveness of self-regulation by determining how many commercial Web sites are providing notice of their information practices and offering consumers choice regarding the collection and use of their personal information online.[97] To that end, in March 1998 Commission staff conducted an online survey of 1,402 commercial Web sites, including 212 sites directed to children.

The survey consists of six samples — group A, drawn from all commercial U.S. sites "likely to be of interest to consumers;" groups B, C, and D, drawn from all such sites in the health, retail, and financial sectors, respectively;[98] group E, drawn from all commercial U.S. sites "primarily directed to children aged fifteen or younger;" and group F, which includes the most popular U.S. commercial sites.[99] There are 674 sites in the Comprehensive Sample (group A), 137 sites in the Health Sample (group B), 142 sites in the Retail Sample (group C), 125 sites in the Financial Sample (group D), 212 sites in the Children's Sample (group E), and 111 sites in the Most Popular Sample (group F). A detailed methodology describing the survey sample selection, data collection, and validation procedures is included in Appendix A. A list of the sites included in each sample is included in Appendix C.

Forty Commission staff members [hereinafter "surfers"] surveyed the sites in each of the samples in the two-week period from March 9-20, 1998. Once a surfer concluded that a site qualified for inclusion in one of the samples (*i.e.*, it was "likely to be of interest to consumers" or was "primarily directed to children aged fifteen or younger"), the surfer searched the site to determine whether it collects personal information from online consumers and, if so, to ascertain

the kinds of information it collects and whether it discloses its information practices.[100] In the case of sites directed to children, personal information collected on a payment form was deemed to be collected from adults; all other personal information sought by children's sites was considered to be collected from children.

For purposes of this survey, "personal information" was defined to include two broad information categories: information that can be used to identify consumers, such as name, postal or e-mail address ("personal identifying information"); and demographic and preference information (such as age, gender, income level, hobbies, or interests) that can be used either in aggregate, non-identifying form for purposes such as market analysis, or in conjunction with personal identifying information to create detailed personal profiles of consumers.

To determine whether Web sites are giving consumers notice of their information practices and offering consumers choice, Commission staff searched Web sites for information practice disclosures. Such disclosures might be found in a "Privacy Policy Notice," defined as a comprehensive description of a site's information practices that is located in one place on the site and may be reached by clicking on an icon or hyperlink. Disclosures might also take the form of a discrete "Information Practice Statement," defined as a statement that describes a particular use or practice regarding consumers' personal information, or regarding a choice offered to consumers about their personal information, that might appear in diverse locations on the site. Examples of such disclosures include statements such as the following:

- We keep all the information you provide us confidential.
- We will only use the information you provide us to process your order.
- We [will, sometimes, never] share your information with third parties.

Staff also counted as an Information Practice Statement any disclosure that did not explicitly state how the personal information collected might be used, but nevertheless arguably raised an inference of at least one potential use. Statements such as "Click here to be on our mailing list" were, therefore, included as Information Practice Statements. Sites in the Children's Sample were analyzed to determine the nature of information collected from children and the extent of notice and/or choice offered to parents. Copies of the survey instructions and survey forms are included

in Appendices B and C, respectively. The survey results are set forth in the survey forms included in Appendix C and in the tables included in Appendix D.

B. GENERAL SURVEY FINDINGS

This section of the report describes the survey results for all sites other than those directed to children. It describes the types of companies whose sites are in each of the four random samples and in the sample of the most popular sites on the Web; the types of personal information collected by these sites; and the frequency and nature of information practice disclosures within each of these samples.

1. WEB SITES

The Comprehensive Sample (Sample A) includes 674 Web sites, and the types of companies included range broadly across the entire spectrum of the American economy. Bookstores, travel agencies and hardware stores, radio and television stations, manufacturers of foods and home health care products, clothing and sports equipment retailers, computer and software developers, online newspapers and magazines, auto dealerships and law firms, and sellers of all manner of other consumer goods and services are included in the Comprehensive Sample. Approximately 37% of the sites in the Comprehensive Sample are operated by small companies (annual sales less than $500,000.00), 40% by medium-sized companies (annual sales exceeding $500,000.00 but less than $10 million), and 20% by large companies (annual sales exceeding $10 million).[101]

The Health, Retail, and Financial Samples (Samples B, C, and D, respectively) are random samples of over 100 sites drawn from industry sectors in which consumers may have heightened concerns for privacy due to the types of personal information such Web sites are likely to collect: health-related sites may collect sensitive medical information; retail sites often collect credit card numbers; and sites offering financial services often collect account and asset-related information.

The Health Sample (Sample B) includes 137 sites operated by drug manufacturers, doctor's offices, hospitals, outpatient clinics, health maintenance organizations, manufacturers and retailers of health care products and non-prescription drugs, sellers of nutritional supplements, weight loss

centers, substance abuse treatment centers, and health information and referral services. Small, medium, and large businesses are nearly equally represented in the Health Sample (32% small; 35% medium-sized; and 31% large).[102]

The Retail and Financial Samples (Samples C and D) are similarly diverse. The range of consumer goods and services sold by the companies represented in the Retail Sample (Sample C) mirrors the variety found in the Comprehensive Sample. Sellers of photographic equipment, automobiles, cigars, jewelry, clothing, computers and software, fine art, collectibles, books, housewares and sheet music are represented, as are magazines, restaurants, sporting goods stores, and pharmacies. Forty percent of the 142 companies in the Retail Sample are small, 37% medium-sized, and 21% large.[103] The Financial Sample (Sample D) includes 125 sites operated by banks, credit unions, mortgage companies, real estate agencies, security and stock brokerages, investment and asset management firms, venture capital firms, investment counselors, stock exchanges, student loan services, and investment newsletters. Eighteen percent of the sites in the Financial Sample are associated with small companies, 41% with medium-sized companies, and 39% with large companies.[104]

The Most Popular Sample (Sample F) includes 111 of the most popular sites on the Web. Companies represented in this sample include search engines, Internet service providers, electronic mail services, software and computer companies, news and information companies, online directories, entertainment companies, and retailers of consumer goods.[105]

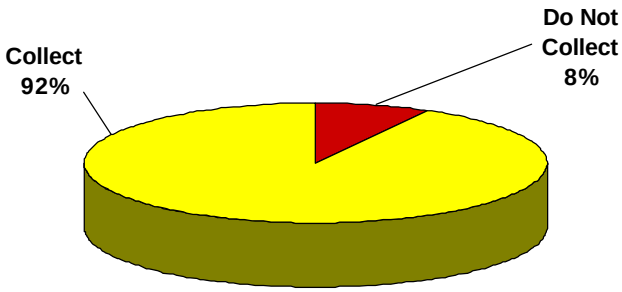
2. PERSONAL INFORMATION COLLECTION

As noted above, in the three years since the Commission's first workshop on online privacy issues, there has been substantial survey research indicating that consumers are concerned that commercial Web sites are collecting a great quantity of personal information online and that this practice might infringe on consumers' privacy.[106] The Commission's own survey findings demonstrate that, indeed, a significant amount of personal information is being collected from online consumers.

As the findings on information collection are consistent across all four random samples and the Most Popular Sample, they are discussed together here. Almost all of the sites in these samples — between 87% and 97% — collect at least one type of personal information from online consumers.[107] The vast majority of sites in all samples collect several types of personal information. Figure 1 shows the percent of sites in the Comprehensive Sample that collect personal information; Figure 1A provides this information for all of the random samples and the Most Popular Sample.

Figure 1

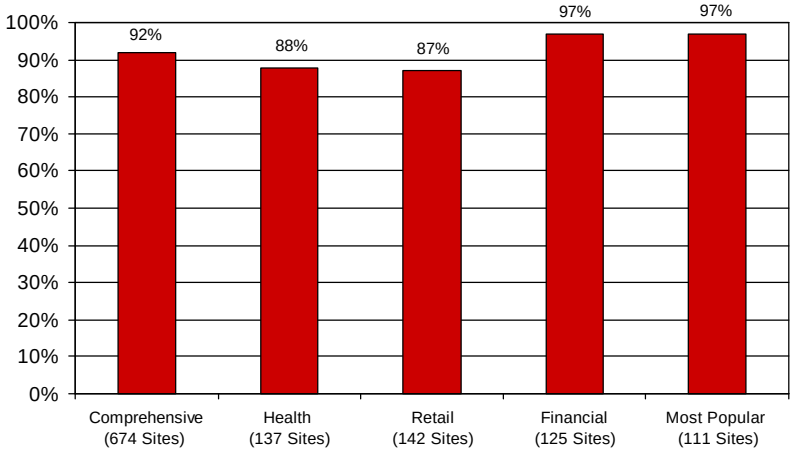
Percent of Web Sites Collecting Personal Information
Comprehensive Sample



Base: All Web Sites in Comprehensive Sample (674) March 1998

Figure 1A

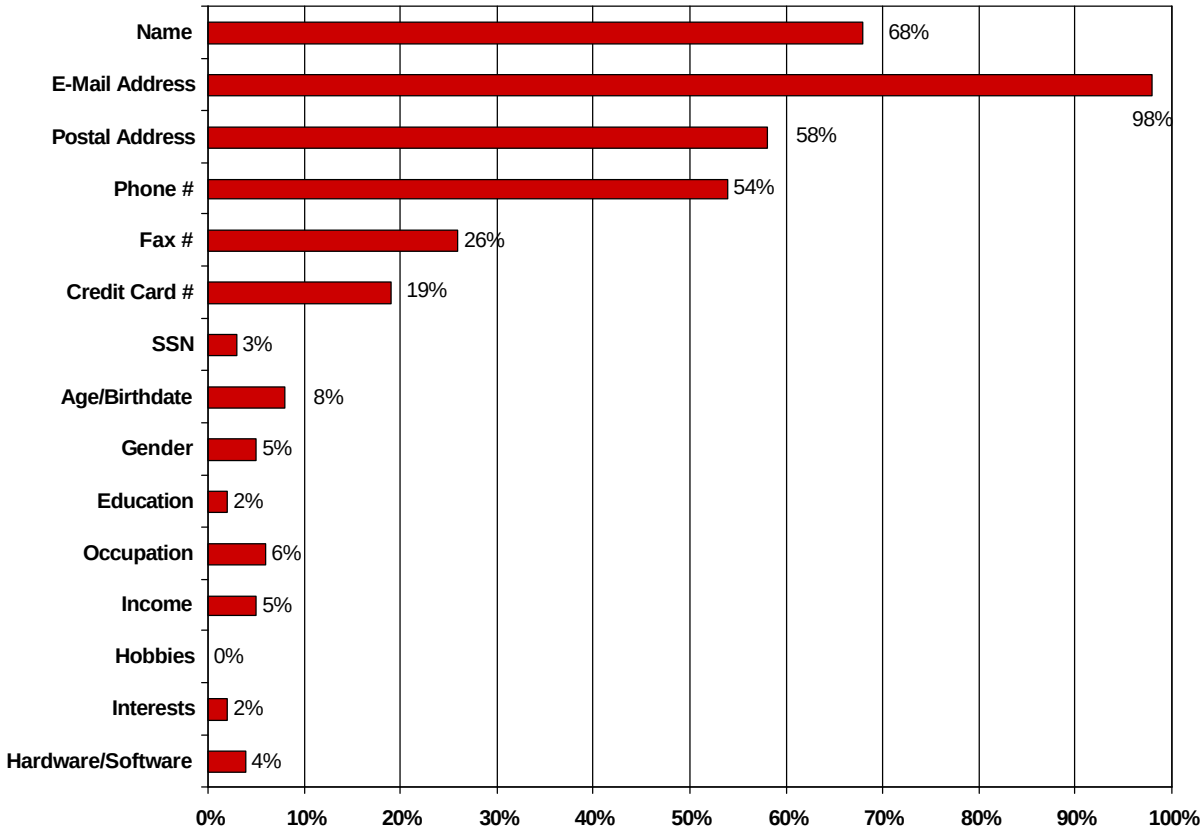
Percent of Web Sites Collecting Personal Information, By Sample



These Web sites collect a remarkable variety of personal information, including name, e-mail address,[108] postal address, telephone number, fax number, credit card number, Social Security number, age or date of birth, gender, education, occupation, income, hobbies, interests, and the type of hardware or software used by the online consumer. Figure 2 shows the percent of sites in the Comprehensive Sample that collect each type of personal information.[109]

Figure 2

Types of Personal Information Collected
Comprehensive Sample

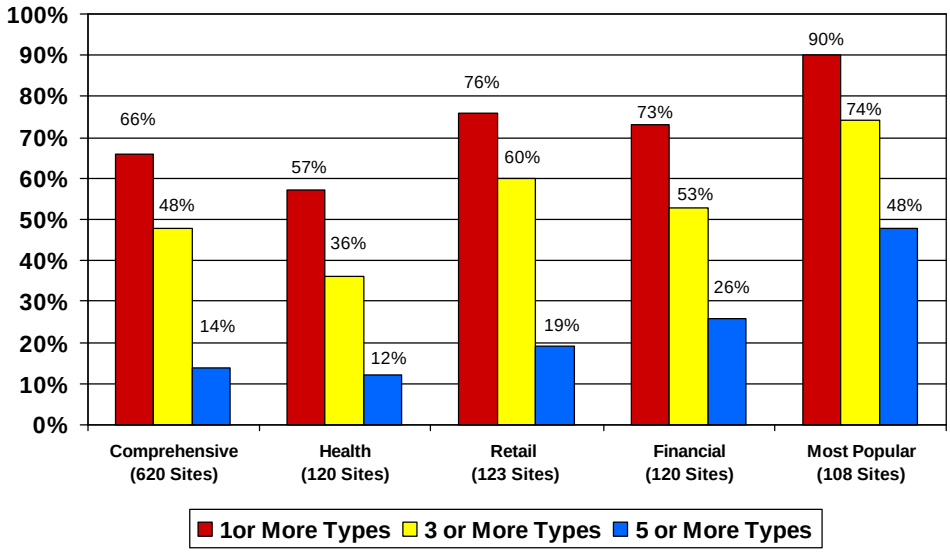


The number of sites in each sample that collect personal identifying information, such as name, e-mail or postal address, credit card number or Social Security number, is also worthy of note.[110] All of the sites in the Health, Retail, and Most Popular Samples that collect personal information, and all but one of such sites in each of the Comprehensive and Financial Samples, collect at least one item of personal identifying information.[111] All of these sites, therefore, are capable of creating personal profiles of online consumers by tying any demographic or interest information they collect to personal identifying information.[112]

Indeed, many of the sites that collect a consumer's name or e-mail address also collect other types of information about the consumer. For example, of those sites in the Comprehensive Sample that collect a consumer's name and/or e-mail address, 14% collect five or more additional types of personal information, 48% collect three or more additional types of personal information, and 66% collect at least one other type of personal information. The numbers in the Most Popular Sample are significantly higher. Of those sites in the Most Popular Sample that collect a consumer's name and/or e-mail address, 48% collect five or more additional types of personal information, 74% collect three or more additional types of personal information, and 90% collect at least one additional type of personal information.[113]

Figure 3

Of those Web Sites that Collect Name and/or E-Mail Address, Percent that Collect One or More Additional Type(s) of Personal Information, By Sample



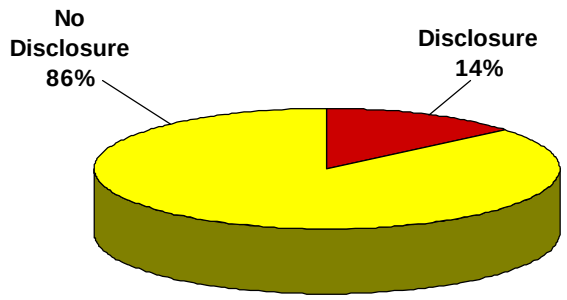
3. FREQUENCY OF DISCLOSURES

a. Random Samples

In contrast to the number of sites that collect personal information, the number of sites in the random samples that have any type of information practice disclosure, *i.e.*, either a Privacy Policy Notice or an Information Practice Statement, is extremely low. This result is consistent across all four of these samples. Only 14% of all sites in the Comprehensive Sample, 14% of all sites in the Health Sample, 13% of all sites in the Retail Sample, and 16% of all sites in the Financial Sample post any disclosure.[114]

Figure 4

Percent of Web Sites with an Information Practice Disclosure
Comprehensive Sample



Base: All Web sites in Comprehensive Sample (674) March 1998

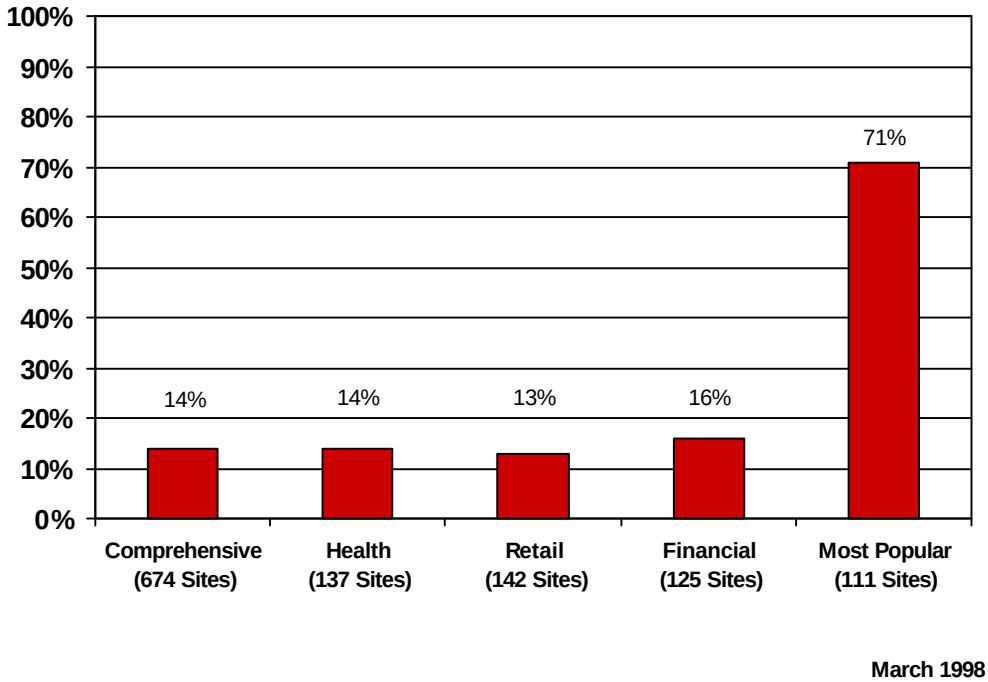
Among sites in the random samples that collect personal information, the disclosure rate is equally low. Of these sites, only 15% in the Comprehensive Sample, 16% in the Health Sample, 15% in the Retail Sample, and 17% in the Financial Sample have any information practice disclosure.[115] Only 2% of the sites that collect personal information in each of these samples have a Privacy Policy Notice.[116] Of sites that collect personal information, 14% in the Comprehensive Sample, 16% in the Health Sample, 13% in the Retail Sample, and 15% in the Financial Sample have at least one Information Practice Statement.[117]

b. Most Popular Sample

The disclosure rate is much higher in the Most Popular Sample (Sample F). Seventy-one percent of all sites have some type of information practice disclosure (either a Privacy Policy Notice or an Information Practice Statement),[118] and 73% of sites that collect personal information have such a disclosure.[119] Of the sites in this sample that collect personal information,

Figure 4A

Percent of Web Sites with an Information Practice Disclosure, By Sample

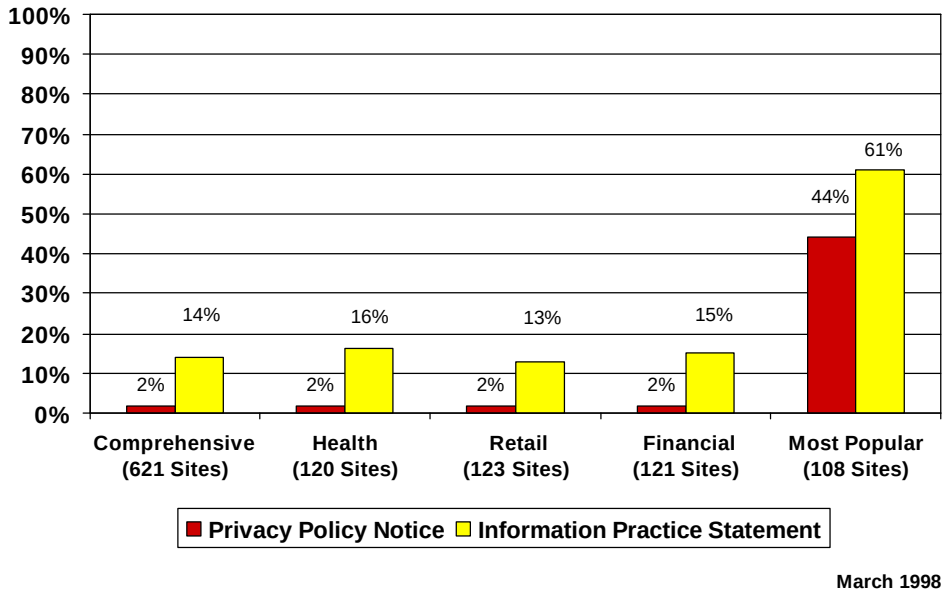


44% have a Privacy Policy Notice,[120] and 61% have at least one Information Practice Statement.[121] The higher disclosure rate for the Most Popular Sample demonstrates that providing notice to consumers is feasible. The higher disclosure rate may be attributable not only to these companies' awareness of online privacy issues, but also to the fact that, of all the sites surveyed for this report, only companies in this sample were on notice that their sites would *all* be

included in the survey, as a result of both press reports and public statements by Commission staff.[122] However, despite this clear public notice, over one-quarter of these sites still failed to post an information practice disclosure.

Figure 5

Of those Web Sites that Collect Personal Information,
Percent with a Privacy Policy Notice or
an Information Practice Statement, By Sample



4. NATURE OF DISCLOSURES

a. Random Samples

As noted above, the disclosure rate for the Comprehensive, Health, Retail, and Financial Samples is very low, ranging between 13% and 16% of all sites. The following discussion of the substance of those disclosures pertains only to those sites in each sample that both collect personal information *and* have at least one information practice disclosure: 94 sites in the Comprehensive Sample; 19 sites in the Health Sample; 18 sites in the Retail Sample; and 20 sites

in the Financial Sample.[123] The small sample size makes it difficult to draw conclusions regarding the nature of disclosures and, therefore, the analysis should be read with the small number of relevant sites in mind.[124]

Roughly one-third of the sites in each of these samples that have at least one information practice disclosure state that they give consumers choice about how the personal information they collect will be used.[125] The percent of sites offering consumers access to their personal information and/or an opportunity to correct any inaccuracies in that information is much lower, ranging from 0% in the Health and Financial Samples to 17% (or 3 sites) in the Retail Sample.[126] The percent of sites that state that they take steps to provide security for the personal information collected after they receive it ranges from 0% in the Health Sample to 15% (or 14 sites) in the Comprehensive Sample.[127]

Staff also gathered data regarding the number of sites whose disclosures address the issue of the potential transfer of personal information to third parties. The percent of sites stating that none of the personal information they collect will be disclosed to third parties ranges from 20% (or 4 sites) in the Financial Sample to 33% (or 31 sites) in the Comprehensive Sample.[128] Twenty-six percent (or 5 sites) of the sites with some information practice disclosure in the Health Sample, 33% (or 6 sites) in the Retail Sample, 36% (or 34 sites) in the Comprehensive Sample, and 40% (or 8 sites) in the Financial Sample state that at least some of the personal information collected may be released to third parties.[129] Only a single site that collects personal information in the Comprehensive Sample — and none of the sites in the other random samples — states that it provides choice, access, and security and addresses the issue of third-party disclosures.[130]

b. Most Popular Sample

The disclosure rate for the most frequently trafficked sites on the Web is, as noted above, significantly higher than the rates for the four random samples. Of the sites in this sample that both collect personal information and have at least one information practice disclosure, 68% (or 54 sites) state that they give consumers choice about how the personal information collected will be used,[131] 38% (or 30 sites) state that they provide consumers access to their personal information and/or an opportunity to correct any inaccuracies in that information,[132] and 16% (or

13 sites) state that they take steps to provide security for the personal information collected after they receive it.[133]

Fourteen percent (or 11 sites) of the sites in this sample that collect personal information and have an information practice disclosure say that none of the personal information they collect will be disclosed to third parties.[134] Seventy-eight percent (or 62 sites) of these sites state that at least some of the personal information collected may be released to third parties.[135] Six percent (or 5 sites) of these sites say that they provide consumers choice, access, and security, and address the issue of third-party disclosures.[136]

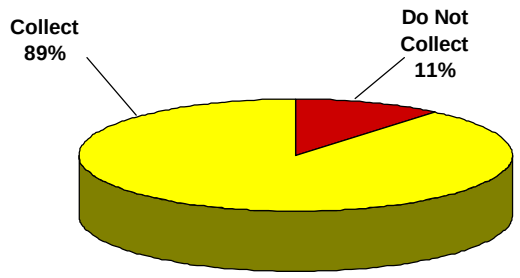
C. CHILDREN'S SURVEY FINDINGS

1. PERSONAL INFORMATION COLLECTION FROM CHILDREN

Commission staff surveyed Web sites in this Sample to ascertain whether they collect personal information from children online, and, if so, to identify the types of information they collect. Staff found that 89% of the 212 sites collect one or more types of personal information from children (a rate comparable to all of the other samples)[137] and that 88% collect at least one type of personal identifying information as well.[138] Personal information collected from children includes a wide array of identifying information such as name, e-mail address,[139] postal address,

Figure 6

Percent of Web Sites Collecting Personal Information from Children

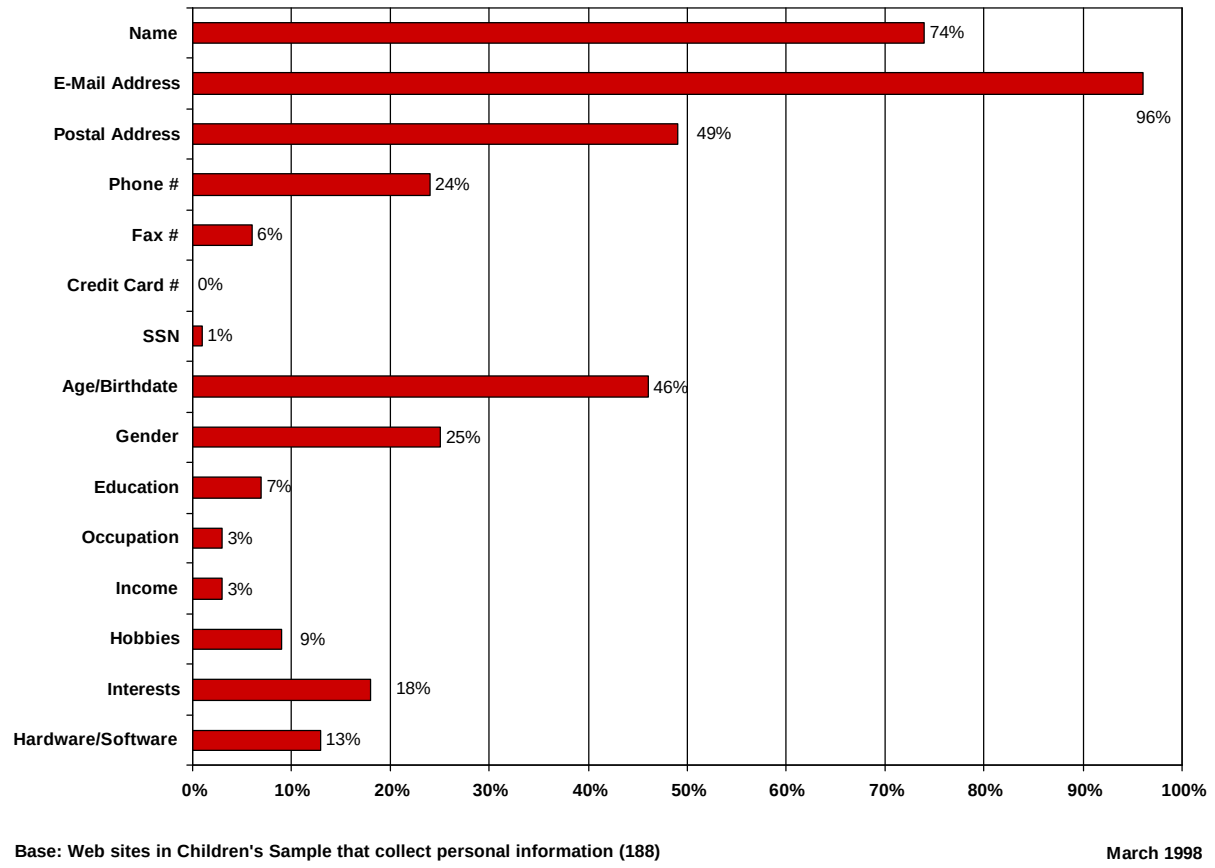


Base: All Web sites in Children's Sample (212) March 1998

telephone number, and Social Security number, as well as other personal information like age or date of birth, gender, education, interests, and hobbies.[140]

Figure 7

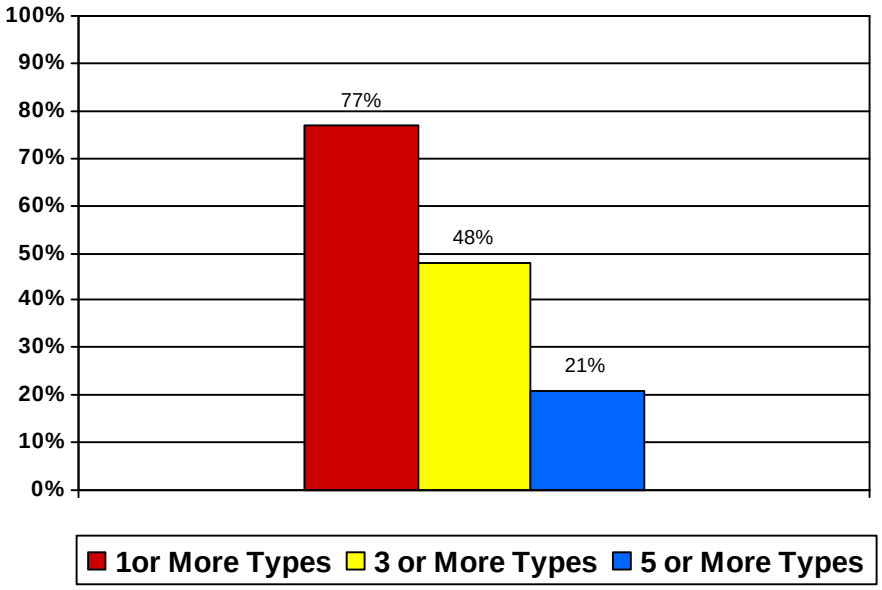
Types of Personal Information Collected from Children



Often the sites that collect personal identifying information also collect several other types of information, enabling them to form a detailed profile of a child. In fact, of the sites that collect a child's name and/or e-mail address, 21% collect five or more additional types of personal information, 48% collect three or more additional types of personal information, and 77% collect one or more additional types of personal information from children.[141]

Figure 8

Of those Web Sites that Collect Name and/or E-Mail Address,
Percent that Collect One or More Additional
Type(s) of Personal Information from Children



Base: Web sites in Children's Sample that collect name and/or e-mail address from children (186) **March 1998**

Web sites use a variety of techniques to solicit personal information from children. For example, some sites require children to answer questions about their interests in order to register or to become eligible to win prizes.[142] In other cases a site may use "imaginary" characters to request information from children, have children sign a "guest book," solicit information to create home pages for children, invite children to participate in chat and electronic pen pal programs, require children to register with the site for updates and information, and offer prizes and other incentives for completing surveys and polls. Some sites use detailed questionnaires, soliciting information about children's age, gender, geographic location, and even personal finances.[143]

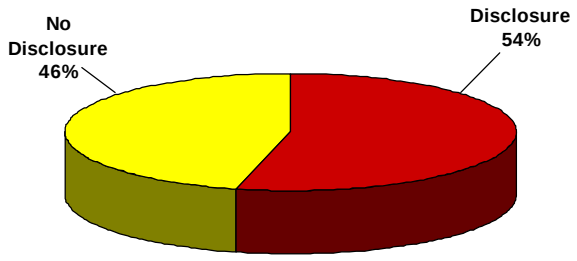
While it was not possible to determine all the purposes for which personal information collected from children is used, many uses were apparent simply from visiting sites. Surfers found, for example, that some sites collect e-mail addresses to send children newsletters and notices about online contests and chances to win prizes on the site. Other sites collect personal information from children to notify them of contest results and to ask children for feedback about the site.

2. FREQUENCY OF DISCLOSURES

The percentage of children's sites providing some degree of disclosure about their collection and use of information was significantly higher than that for all samples other than the Most Popular Sample.[144] Fifty-four percent of all sites in the Children's Sample have some kind of information practice disclosure, either a comprehensive Privacy Policy Notice or at least one Information Practice Statement, or both.[145]

Figure 9

Percent of Children's Web Sites
with an Information Practice Disclosure



Base: All Web sites in Children's Sample (212) March 1998

As noted above with respect to the general samples, staff applied a very broad definition of what constitutes an Information Practice Statement. Any statement that describes a particular use or practice regarding consumers' personal information and/or a choice offered to consumers about their personal information was considered an Information Practice Statement. Examples from the Children's Sample include statements such as:

- C Kids, get your parents' permission before you give out information online;
- C We reserve the right to do whatever we want with the information we collect, and

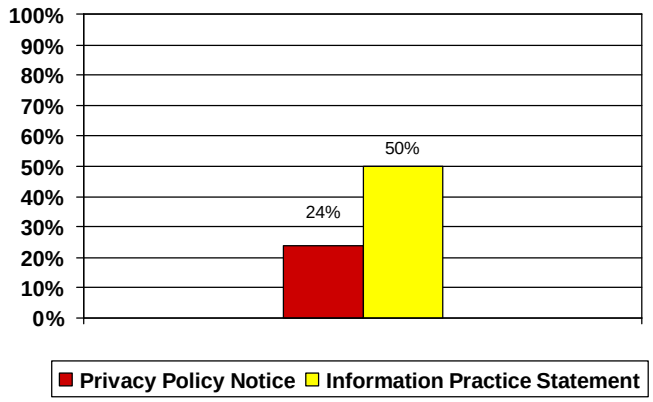
C Click here if you want to be on our mailing list.

Of sites that collect personal information from children, 50% have at least one Information Practice Statement.[146]

Although a majority of children's sites have some statement about one or more of their information practice(s), the number of children's sites that have a Privacy Policy Notice is much lower. Twenty-four percent of the sites that collect personal information from children post a Privacy Policy Notice.[147]

Figure 10

Of those Web Sites that Collect Personal Information from Children, Percent with a Privacy Policy Notice or an Information Practice Statement



Base: Web sites in Children's Sample that collect personal information (188)

March 1998

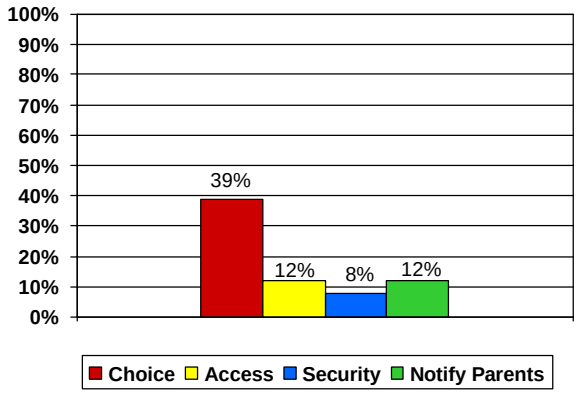
3. NATURE OF DISCLOSURES

The following discussion of the nature of disclosures by sites in the Children's Sample applies only to those sites that both collect personal information from children and have at least one information practice disclosure (109 sites). Thirty-nine percent (or 43 sites) of these sites say

that they provide children or their parents with choices about how their personal information will be used.[148] Only 12% (or 13 sites) of these sites say that they offer access to this personal information or an opportunity to correct inaccuracies.[149] The percentage of sites that state they take steps to provide security for personal information after they receive it is lower still — 8% (or 9 sites).[150] Only 12% (or 13 sites) say they will notify parents of their information practices. Of the sites that collect personal information from children and have at least one information practice disclosure, no site's information practice disclosure discusses the full range of fair information practice principles — choice, access, security *and* parental notice.

Figure 11

Of those Sites that Collect Personal Information from Children and Have an Information Practice Disclosure, Percent that Offer Choice, Access, Security and/or Notify Parents of Information Practices



Base: Web sites in Children's Sample that collect personal information from children and have an Information Practice Disclosure (109)

March 1998

The survey also shows that numerous sites disclose children's personal information to third parties. There are two ways that sites disclose personal information to third parties: (1) sites may display children's personal information in areas accessible to anyone online; or (2) sites may sell or rent children's personal information to others. In either case, the release of children's personal

identifying information to third parties is of concern, because it creates a risk of injury to or exploitation of children so identified. As described earlier, 97% of parents are concerned about whether their children's personal information is shared with third parties.[151] Despite parents' concern, staff found sites, for example, that display color photographs of young children with their full names and ages, as well as sites that facilitate public disclosure of children's e-mail addresses in bulletin boards, chat rooms, "art galleries," and on children's home pages.

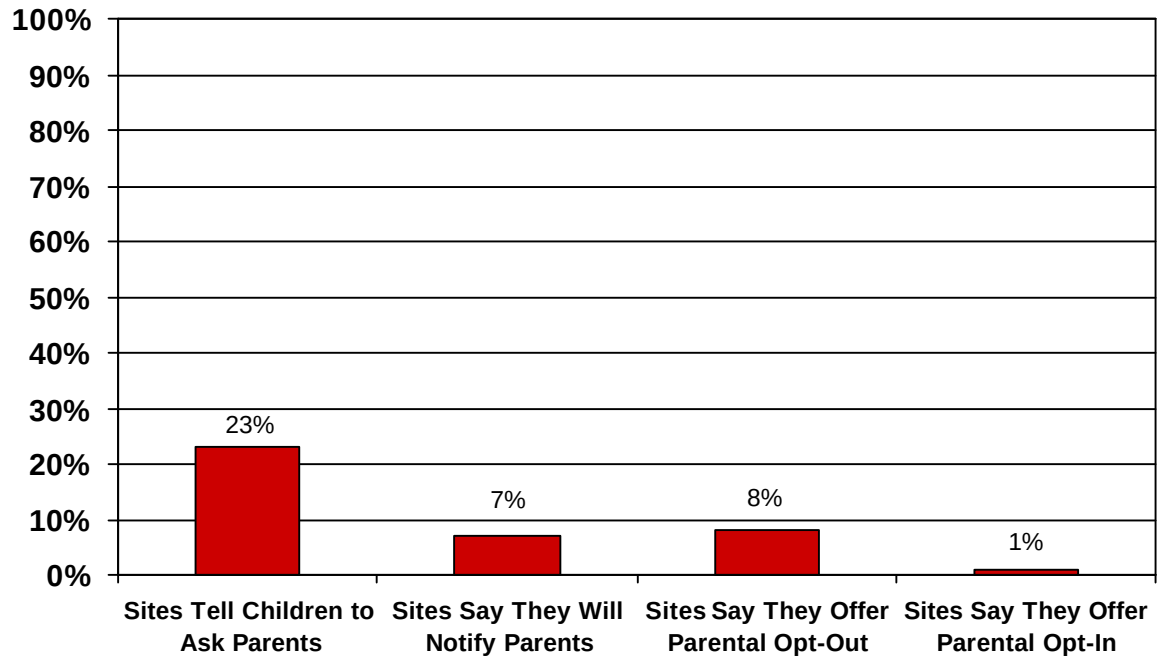
Of those sites that collect personal information from children and have an information practice disclosure, 82% have some kind of disclosure stating whether or not children's information will be publicly posted or otherwise shared with third parties.[152] Only 33% have an information practice disclosure stating that *none* of the information will be released to third parties.[153] Forty-nine percent say that the information *may* be released to third parties.[154]

4. PARENTAL INVOLVEMENT

The role of parents in protecting their children's privacy is fundamental to the implementation of the fair information practice principles described in this report, and is the principle touchstone of both the staff opinion letter and the CARU guidelines. The survey percentages were low with regard to parental control over the collection and use of information. Only 23% (or 48 sites) of all the sites in the Children's Sample take the first step of telling children to ask their parents for permission before providing information to the site.[155] Less than 8% of the sites say they notify parents of their information practices.[156] Only 1% (or 3 sites) require parental consent to the collection and use of information *before* the information is collected or used (opt-in)[157] and only 8% (or 17 sites) say that parents can ask that personal information collected from children be deleted or not used in the future (opt-out).[158]

Figure 12

Percent of Web Sites with Disclosures
Regarding Parental Involvement



Base: All Web sites in Children's Sample (212) **March 1998**

The results reveal a very low level of compliance with the basic parental control principles contained in the staff opinion letter and the CARU guidelines more than seven months after these documents were released. First, the results demonstrate that a significant percentage of sites continue to collect a vast array of personal information from children, in sharp contrast to parents' preferences.[159] Second, despite the fact that Commission staff publicly disclosed that the Children's Sample would be selected from sites listed in the Yahooligans! Directory, nearly half of the sample failed to post any kind of information practice disclosure. Finally, very few sites tell children to ask their parents for permission before providing personal information, and fewer still notify parents of their information practices or appear to take any steps to involve parents.

VI. CONCLUSIONS

C A medical clinic's online doctor-referral service invites consumers to submit their name, postal address, e-mail address, insurance company, any comments concerning their medical problems, and to indicate whether they wish to receive information on any of a number of topics, including urinary incontinence, hypertension, cholesterol, prostate cancer, and diabetes. The online application for the clinic's health education membership program asks consumers to submit their name, address, telephone number, date of birth, marital status, gender, insurance company, and the date and location of their last hospitalization. The clinic's Web site says nothing about how the information consumers provide will be used or whether it will be made available to third parties.

C An automobile dealership's Web site offers help to consumers in rebuilding their credit ratings. To take advantage of this offer, consumers are urged to provide their name, address, Social Security number, and telephone number through the Web site's online information form. The Web site says nothing about how the information provided will be used or whether it will be made available to third parties.

C A mortgage company operates an online prequalification service for home loans. The online application form requires that each potential borrower provide his or her name, Social Security number, home and business telephone numbers, e-mail address, previous address, type of loan sought, current and former employer's name and address, length of employment, income, sources of funds to be applied toward closing, and approximate total in savings. The online form also requires the borrower to provide information about his or her credit history, including credit card, car loans, child support and other indebtedness, and to state whether he or she has ever filed for bankruptcy. The application form requires the borrower to agree that the mortgage company may disclose his or her "credit experiences" to third parties, but the Web site says nothing else about how the mortgage company might use all of the information provided or whether that information will be made available to third parties.

C A child-directed site collects personal information, such as a child's full name, postal address, e-mail address, gender, and age. The Web site also asks a child extensive personal finance questions, such as whether a child has received gifts in the form of stocks, cash, savings bonds, mutual funds, or certificates of deposit; who has given a child these gifts; whether a child puts monetary gifts into mutual funds, stocks or bonds; and whether a child's parents own mutual funds. Elsewhere on the Web site, contest winners' full names, age, city, state, and zip code are posted. The Web site does not tell children to ask their parents for permission before providing personal

information and does not appear to take any steps to involve parents. Further, the Web site says nothing about whether the information is disclosed to third parties.

C Another child-directed site collects personal information to register for a chat room, including a child's full name, e-mail address, city, state, gender, age, and hobbies. The Web site has a lotto contest that asks for a child's full name and e-mail address. Lotto contest winners' full names are posted on the site. For children who wish to find an electronic pen pal, the site offers a bulletin board service that posts messages, including children's e-mail addresses. While the Web site says it asks *children* to post messages if they are looking for a pen pal, in fact, anyone of any age can visit this bulletin board and contact a child directly. The site also has an area where children can submit stories online. The Web site posts the stories along with children's full names, ages, and e-mail addresses. The Web site does not tell children to ask their parents for permission before providing personal information and does not say that it takes steps to involve parents. The Web site says nothing about whether the information is disclosed to third parties.

* * *

The practices of these Web sites demonstrate the real need for implementing the basic fair information practices described in this report. The World Wide Web provides a host of opportunities for businesses to gather a vast array of personal information from and about consumers, including children. The online environment and the advent of the computer age also provide unprecedented opportunities for the compilation, analysis, and dissemination of such information. While American businesses have always collected some information from consumers in order to facilitate transactions, the Internet allows for the efficient, inexpensive collection of a vast amount of information. It is the prevalence, ease, and relative low cost of such information collection that distinguishes the online environment from more traditional means of commerce and information collection and thus raises consumer concerns.

The federal government currently has limited authority over the collection and dissemination of personal data collected online.[160] The Federal Trade Commission Act (the "FTC Act" or "Act")[161] prohibits unfair and deceptive practices in and affecting commerce. The Act authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of

the Act, and provides a basis for government enforcement of certain fair information practices. For instance, failure to comply with stated information practices may constitute a deceptive practice in certain circumstances, and the Commission would have authority to pursue the remedies available under the Act for such violations. Furthermore, in certain circumstances, information practices may be inherently deceptive or unfair, regardless of whether the entity has publicly adopted any fair information practice policies. As discussed above, Commission staff has issued an opinion letter addressing the possible unfairness inherent in collecting certain personal identifying information from children online and transferring it to third parties without obtaining *prior* parental consent.[162] However, as a general matter, the Commission lacks authority to require firms to adopt information practice policies.

The Commission has encouraged industry to address consumer concerns regarding online privacy through self-regulation. The Internet is a rapidly changing marketplace. Effective self-regulation remains desirable because it allows firms to respond quickly to technological changes and employ new technologies to protect consumer privacy. Accordingly, a private-sector response to consumer concerns that incorporates widely-accepted fair information practices and provides for effective enforcement mechanisms could afford consumers adequate privacy protection. To date, however, the Commission has not seen an effective self-regulatory system emerge.

As evidenced by the Commission's survey results, and despite the Commission's three-year privacy initiative supporting a self-regulatory response to consumers' privacy concerns, the vast majority of online businesses have yet to adopt even the most fundamental fair information practice (notice/awareness). Moreover, the trade association guidelines submitted to the Commission do not reflect industry acceptance of the basic fair information practice principles. In addition, the guidelines, with limited exception, contain none of the enforcement mechanisms needed for an effective self-regulatory regime. In light of the lack of notice regarding information practices on the World Wide Web and the lack of current industry guidelines adequate to establish an effective self-regulatory regime, the question is what additional incentives are required in order to encourage effective self-regulatory efforts by industry. The Commission currently is

considering this question in light of the survey results, monitoring self-regulation efforts since the survey was completed, and assessing the utility and effectiveness of different courses of action. This summer, the Commission will make recommendations on actions it deems necessary to protect online consumers generally.

In the specific area of children's online privacy, however, the Commission now recommends that Congress develop legislation placing parents in control of the online collection and use of personal information from their children. Such legislation would set out the basic standards of practice governing the online collection and use of information from children. All commercial Web sites directed to children would be required to comply with these standards.

In making this recommendation, the Commission has drawn on its extensive experience in addressing business practices affecting children, as well as its three-year study of online privacy issues. The Commission has already taken some steps, particularly the release of the staff opinion letter, to address online information practices involving children that may violate Section 5 of the Federal Trade Commission Act. Moreover, the Commission has recognized a growing consensus reflected in consumer survey evidence and some industry self-regulatory guidelines that parental involvement is necessary in the collection and use of information from children. Nonetheless, Section 5 may only have application to some but not all of the practices that raise concern about the online collection and use of information from children. The Commission does not believe, for example, that Section 5 necessarily authorizes it to require parental notice and involvement across the board for all commercial Web sites engaged in information collection from children. Accordingly, the Commission concludes that as a matter of policy additional steps should now be taken to ensure adequate online privacy protections for children.

Children's privacy legislation also would recognize that a marketer's responsibilities vary with the age of the child from whom personal information is sought. In a commercial context, Congress and industry self-regulatory bodies traditionally have distinguished between children aged 12 and under, who are particularly vulnerable to overreaching by marketers, and children over the age of 12, for whom strong, but more flexible protections may be appropriate. In each

case, the goal of legislative requirements should be to recognize the parents' role with respect to information collection from children.

Accordingly, the Commission recommends that Congress develop legislation to require commercial Web sites that collect personal identifying information from children 12 and under to provide actual notice to the parent and obtain parental consent as follows:

- Where the personal identifying information would enable someone to contact a child **offline**, the company must obtain *prior parental consent*, regardless of the intended use of the information (opt-in);
- Where the personal identifying information is **publicly posted or disclosed to third parties**, the company must obtain *prior parental consent* (opt-in)*;*
- Where collection of an e-mail address is necessary for a child's participation at a site, such as to notify contest winners, the company must provide *notice* to parents and an opportunity to remove the e-mail address from the site's database (opt-out).

Where the personal identifying information is collected from children over 12, the Commission recommends that:

- Web sites must provide parents with notice of the collection of such information and an opportunity to remove the information from the site's database (opt-out).[163]

The development of the online marketplace is at a critical juncture. If growing consumer concerns about online privacy are not addressed, electronic commerce will not reach its full potential. To date, industry has had only limited success in implementing fair information practices and adopting self-regulatory regimes with respect to the online collection, use, and dissemination of personal information. Accordingly, the Commission now recommends legislation to protect children online and this summer will recommend an appropriate response to protect the privacy of all online consumers.

ENDNOTES

1. In July 1997 the Commission promised that it would submit this report in June 1998. Commission letter to Senator John McCain, Chairman, Committee on Commerce, Science and Transportation, United States Senate (July 31, 1997); Commission Letter to Representative Thomas Bliley, Chairman, Committee on Commerce, United States House of Representatives (July 31, 1997) (hereinafter referred to as "McCain/Bliley letters"). The text of the McCain/Bliley letters may be found on the Commission's Web site at http://www.ftc.gov/os/9707/privac97.htm.

2. The Commission's Public Workshop on Consumer Information Privacy ("1997 Workshop"), June 10-13, 1997, also explored the privacy issues raised by computerized databases that contain consumers' personal identifying information (also known as "individual reference services" or "look-up" services), as well as issues relating to unsolicited commercial e-mail. The workshop transcript may be found on the Commission's Web site at http://www.ftc.gov/bcp/privacy/wkshp97/index.html.

3. These Commission efforts have served as a foundation for dialogue among members of the information industry and online business community, government representatives, privacy and consumer advocates, and experts in interactive technology. The Commission and its staff have also issued reports describing various consumer privacy concerns in the electronic marketplace. *E.g.*, FTC Report to Congress: *Individual Reference Services*, December 1997, available on the Commission's Web site at http://www.ftc.gov/bcp/privacy/wkshp97/index.html [hereinafter "*FTC Report to Congress/Reference Services*"]; FTC Staff Report: *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, December 1996, available at http://www.ftc.gov/reports/privacy/privacy1.htm [hereinafter "*FTC Staff Report*"]; FTC Staff Report: *Anticipating the 21st Century: Consumer Protection Policy in the New High-Tech, Global Marketplace*, May 1996, available at http://www.ftc.gov/opp/global.htm. In addition, the Commission presented testimony on the Implications of Emerging Electronic Payment Systems on Individual Privacy on September 18, 1997 before the House Subcommittee on Financial Institutions and Consumer Credit, Committee on Banking and Financial Services (available at http://www.ftc.gov/os/9709/elecpay.tes.htm); and on Internet Privacy on March 26, 1998 before the House Subcommittee on Courts and Intellectual Property, Committee on the Judiciary (available at http://www.ftc.gov/os/9803/privacy.htm).

4. "Cookie" technology allows a Web site's server to place information about a consumer's visits to the site on the consumer's computer in a text file that only the Web site's server can read. Using cookies a Web site assigns each consumer a unique identifier (not the actual identity of the consumer), so that the consumer may be recognized in subsequent visits to the site. On each return visit, the site can call up user-specific information, which could include the consumer's preferences or interests, as indicated by documents the consumer accessed in prior visits or items

the consumer clicked on while in the site. Web sites can also collect information about consumers through hidden electronic navigational software that captures information about site visits, including Web pages visited and information downloaded, the types of browser used, and the referring Web sites' Internet addresses. Staff did not ascertain whether sites in the Commission's online survey use cookies, or other hidden electronic means, to collect personal information, but looked instead to sites' information practice disclosures to reveal such practices. *See infra* Section V.A and Appendix A.

5. CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Spring '97 (March 12, 1997) (defining adults as individuals over 16 years old), available at http://www.commerce.net/work/pilot/nielsen_96/press_97.html [hereinafter *CommerceNet/Nielsen Demographic Study*, Spring '97]; IntelliQuest Communications, Inc., *Worldwide Internet/Online Tracking Service (WWITS ™): Second Quarter 1997 Study* (Sept. 4, 1997), available at http://www.intelliquest.com/about/release32.htm.

6. *CommerceNet/Nielsen Demographic Study*, Spring '97.

7. CommerceNet and Nielsen Media Research, *CommerceNet/Nielsen Media Demographic and Electronic Commerce Study*, Fall '97 (December 11, 1997), available at http://www.commerce.net/news/press/121197.html [hereafter *CommerceNet/Nielsen Demographic Study*, Fall '97]. *See also* Yankelovich Partners, *1997 Cybercitizen Report* (Mar. 27, 1997) (finding that 23% of users ordered and paid for a product over the Internet, *i.e.*, "transacted" business online), available at http://www.yankelovich.com/pr/970327.htm.

8. Jupiter Communications, *1998 Online Advertising Report* (Aug. 22, 1997) (figure includes directory listings and classified advertisements), available at http://www.jup.com/digest/082297/advert.shtml.

9. Louis Harris & Associates and Dr. Alan F. Westin, *Commerce, Communication, and Privacy Online, A National Survey of Computer Users* (1997) (hereinafter referred to as "*Westin Survey*") at ix.

The Commission recognizes that the widespread availability of consumers' personal information, and the privacy concerns raised thereby, are not unique to the Internet. The Commission has focussed on online privacy for several reasons. First, interactive media make it possible to collect, store, aggregate, and disseminate personal information with speed and efficiency that are unmatched in other contexts. Second, the fact that the online marketplace is in its infancy makes it possible to address online privacy issues prospectively. Finally, and most important, consumers' concerns about their privacy are significantly heightened in the online environment.

10. *Id.* at 20-21.

11. *Business Week/Harris Poll: Online Insecurity*, Business Week, March 16, 1998, at 102.

12. Privacy & American Business Report, Vol. 4, No. 3 (1997) (reporting on Louis Harris Associates and Alan F. Westin's *National Survey of Computer Users*).

13. As the Commission's expertise and regulatory authority relate to commercial activities, its review of children's online privacy issues has focused on the information practices of commercial Web sites. The collection of information from and about children by non-commercial sites such as those operated by non-profit and educational entities, however, raises similar privacy concerns.

14. Interactive Consumers Research Report, Vol. 4, No. 5 at 1, 4, May 1997 (discussing results of FIND/SVP's 1997 American Internet User Survey).

15. *Id*. at 3. The Find/SVP's survey regarding children's online activities reports that approximately 57% of households with online children use the Internet for homework and school-related research (64% with children ages 8 to 11); 51% use it for entertainment or games (78% with children ages 8 to 11); 45% use it for surfing or browsing (60% with children ages 8 to 11); 37% use it for e-mail and chat (35% with children ages 8 to 11); and 43% use it for informal learning (59% with children ages 8 to 11).

16. *Id*. at 1, 2. The number of children online increased nearly five-fold from fall 1995 to spring 1997. *Id.* at 1.

17. One source has estimated that, in 1997, children aged 4 through 12 spent $24.4 billion themselves; and children aged 2 through 14 may have directly influenced spending by their parents in an amount as much as $188 billion. James U. McNeal, *Tapping the Three Kids' Markets*, American Demographics, Apr. 1998, at 38, 40.

18. According to one source, most children's Web sites are targeting children ages 8 to 11. Teens tend to visit the same sites that adults visit. Robin Raskin, *What do Kids Want?*, Family PC Magazine, May 1998, at 17.

19. The types of personal information include personal identifying information, such as name, e-mail address, phone number, and home address, as well as other personal information such as the child's age, gender, hobbies, interests, favorite foods, games, movies, books, and animated characters. *See infra* Section V. C. 1.

20. *See FTC Staff Report*, Appendix E.

21. The "Innocent Images" program focuses on individuals who go online to meet children for the purpose of engaging in sexual activity or who produce and/or distribute child pornography online. *See* 1997 Workshop, Transcript at 229 (testimony of FBI agent Linda Hooper). *See also* Testimony of Louis J. Freeh, Director, Federal Bureau of Investigation, before the Senate

Appropriations Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, March 10, 1998, available at http://www.fbi.gov/congress/internet/sac310.htm; and Testimony of Stephen R. Wiley, Chief, FBI Violent Crime and Major Offenders Section, before the House Subcommittee on Crime, Committee on the Judiciary, November 7, 1997, available at http://www.fbi.gov/congress/children/children.htm.

22. 1997 Workshop, Transcript at 192-93 (testimony of Charlotte Baecher of Consumers Union).

23. *Id.* at 36-37.

24. *Id.*

25. *Id.*

26. *Id.* at 156 (testimony of Alan Westin).

27. Fair information practice principles were first articulated in a comprehensive manner in the United States Department of Health, Education and Welfare's seminal 1973 report entitled *Records, Computers and the Rights of Citizens* (1973) [hereinafter "HEW Report"]. In the twenty-five years that have elapsed since the HEW Report, a canon of fair information practice principles has been developed by a variety of governmental and inter-governmental agencies. In addition to the HEW Report, the major reports setting forth the core fair information practice principles are: The Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977) [hereinafter "*Privacy Protection Study*"]; Organization for Economic Cooperation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) [hereinafter "*OECD Guidelines*"]; Information Infrastructure Task Force, Information Policy Committee, Privacy Working Group, *Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information* (1995) [hereinafter "*IITF Report*"]; U.S. Dept. of Commerce, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (1995) [hereinafter "*Commerce Report*"]; *The European Union Directive on the Protection of Personal Data* (1995) [hereinafter "*EU Directive*"]; and the Canadian Standards Association, *Model Code for the Protection of Personal Information: A National Standard of Canada* (1996) [hereinafter "*CSA Model Code*"]. Other sources relied upon herein include the *FTC Staff Report* and *FTC Report to Congress/Reference Services.*

28. Such principles can be either procedural or substantive. Procedural principles address how personal information is collected and used by governing the methods by which data collectors and data providers interact. These principles ensure that consumers have notice of, and consent to, an entity's information practices. Substantive principles, by contrast, impose substantive limitations on the collection and use of personal information, regardless of consumer consent, by requiring

that only certain information be collected and that such information only be used in certain ways. Most of the principles discussed below are procedural in nature. One substantive principle widely adopted by the fair information practice codes, but not discussed below, is the collection limitation principle, which states that entities should only collect personal information necessary for a legitimate business purpose. *See Privacy Protection Study* at 513-15; *IITF Report* § II.A; *CSA Model Code* ¶ 4.4.

29. *See, e.g.*, *OECD Guidelines*, *Explanatory Memorandum* ¶ 52; *see also FTC Staff Report* at 9.

30. While notice of a Web site's policies with respect to data integrity and security is critical to making an informed decision to reveal personal data, such notice is not a prerequisite to the implementation of security measures. The implementation of security measures lies solely in the hands of the entity collecting the information and requires no active participation from the consumer. Implementation of the principles of choice and access, by contrast, require consumer involvement and, therefore, are dependent on notice to be meaningful.

31. *OECD Guidelines*, Openness Principle & ¶ 12; *FTC Staff Report* at 9-10; *EU Directive* art. 10; *CSA Model Code* ¶ 4.8.2.

32. *HEW Report* at 62; *Privacy Protection Study* at 514; *OECD Guidelines*, Purpose Specification Principle & ¶ 9; *IITF Report* § II.B.; *Commerce Report* at 21; *EU Directive* art. 10; *CSA Model Code* ¶ 4.2; *FTC Staff Report* at 9-10. The corollary to identifying the purposes for data collection is that the data not be used for other purposes without the data subject's consent. *See HEW Report* at 61-62; *OECD Guidelines*, Use Limitation Principle & ¶ 10 and *Explanatory Memorandum* ¶ 55; *IITF Report* § II.D; *EU Directive* arts. 6-7; *CSA Model Code* ¶ 4.5.

33. *EU Directive* art. 10.

34. *Commerce Report* at 21.

35. *HEW Report* at 59; *IITF Report* § II.B; *EU Directive* art. 10. Several of the fair information practice codes recognize that a consumer's refusal to allow the further unrelated use of his or her personal information, beyond that which is necessary to complete the transaction at issue, should not form the basis for the denial of access to the good or service in question. *See, e.g.*, *Commerce Report* at 25; *CSA Model Code* ¶ 4.3.3.

36. *Privacy Protection Study* at 514; *IITF Report* § II.B. As noted in endnote 30, notice of this type is not a prerequisite to insuring the confidentiality, integrity, and quality of data. However, when dealing with data considered by consumers to be particularly sensitive, information about the steps taken by the data collector is important to the consumer and may determine whether the consumer is willing to provide such data.

37. *See FTC Staff Report* at 9-10.

38. *HEW Report* at 58; *CSA Model Code* ¶ 4.8.2; *EU Directive* art. 10.

39. *HEW Report* at 58; *EU Directive* art. 10.

40. *IITF Report* § II.B.

41. *Cf. CSA Model Code* ¶ 4.8.2 (organizations should make available identity of individual accountable for organization's policies and to whom complaints can be forwarded).

42. Virtually every set of fair information practice principles includes consumer choice or consent as an essential element. *HEW Report* at 41, 61; *OECD Guidelines*, Collection Limitation Principle & ¶ 7 and Use Limitation Principle & ¶ 10; *Commerce Report* at 23-27; *EU Directive* arts. 7, 14; *CSA Model Code*, ¶¶ 4.3, 4.5; *see also FTC Report to Congress/Reference Services* at 22-23; *FTC Staff Report* at 10-11.

43. As noted in the FTC Staff Report, commentators have taken different views of the efficacy and wisdom of opt-in versus opt-out regimes. *FTC Staff Report* at 10-11; *see also Commerce Report* at 24-27 (proposing opt-in regimes for "sensitive information" and opt-out regimes for other information).

44. Indeed, technological innovations soon may allow consumers and collectors of information to engage in "electronic negotiation" regarding the scope of information disclosure and use. Such "negotiation" would be based on electronic matching of pre-programmed consumer preferences with Web sites' information practices. The World Wide Web Consortium ("W3C") is currently in the final stages of developing its Platform for Privacy Preferences Project ("P3P"), which will allow implementation of such technology. Consumers may have access to P3P by early 1999. For general information on P3P, see the W3C's Web site (http://www.w3.org/P3P).

45. A system requiring consumers to specify privacy preferences before visiting any Web sites can be built into Internet browsers. *See supra* note 44 (discussing technological developments). The absence of default rules, and the concomitant requirement that consumers decide how they want their personal information used, help ensure that consumers in fact exercise choice.

46. *See HEW Report* at 41, 59, 63; *Privacy Protection Study* at 508-13; *OECD Guidelines*, Individual Participation Principle & ¶ 13; *IITF Report* § III.B; EU Directive art. 12; *CSA Model Code* ¶ 4.9; *FTC Report to Congress/Reference Services* at 21-22. *See also* Fair Credit Reporting Act ("FCRA") §§ 609-11, 15 U.S.C. §§ 1681g-1681i (providing for consumer access to, and the right to correct inaccuracies in, consumer credit reports).

47. *See HEW Report* at 63; *IITF Report* § III.B; *CSA Model Code* ¶ 4.9; *OECD Guidelines*, Individual Participation Principle & ¶ 13 and *Explanatory Memorandum* ¶ 61; *EU Directive* art. 12; *see also FTC Report to Congress/Reference Services* at 21-22; FCRA § 611, 15 U.S.C. § 1681i.

48. *HEW Report* at 56-57; *Privacy Protection Study* at 521; *OECD Guidelines*, Data Quality Principle & ¶ 8 and *Explanatory Memorandum* ¶ 53; *IITF Report* § I.C; *EU Directive* art. 6; *CSA Model Code* ¶¶ 4.5.3, 4.6; *see also* FCRA §§ 605, 607(b), 15 U.S.C. §§ 1681c, 1681e(b).

49. *OECD Guidelines*, Security Safeguards Principle & ¶ 11 and Explanatory Memorandum ¶ 56; *IITF Report* §§ I.B, II.C; *EU Directive* art. 17; CSA Model Code ¶ 4.7; *FTC Staff Report* at 12. Physical security measures, such as guards, alarms, etc., may also be necessary in certain circumstances.

50. In implementing security measures, companies should be aware that security breaches directed at *stored* data — *i.e.*, information already received by the data collector — often constitute greater threats to privacy than those breaches occurring during the *transmission* of sensitive data, such as credit card numbers, over the Internet. *See, e.g.*, Linda Punch, *The Real Internet Security Issue*, Credit Card Management, Dec. 1997, at 65.

51. *See HEW Report* at 50 (calling for Code of Fair Information Practices that includes civil and criminal penalties, the availability of injunctive relief, and individual rights of action for actual, liquidated, and punitive damages); *OECD Guidelines*, Accountability Principle & ¶14 and *Explanatory Memorandum* ¶ 62 (accountability supported by legal sanctions); *IITF Report* § III.C ("envision[ing] various forms [of redress] including . . . informal complaint resolution, mediation, arbitration, civil litigation . . . ."); *EU Directive* arts. 22-23 (judicial remedy and compensation).

52. *Cf. Privacy Protection Study* at 33 (identifying voluntary compliance, statutorily-created rights enforceable through individual or government action, and centralized government mechanisms as means of implementing compliance).

53. The European Union ("EU") has recognized that self-regulation may in certain circumstances constitute "adequate" privacy protection for purposes of the EU Directive's ban on data transfer to countries lacking "adequate" safeguards. *See EU Directive* art. 25. The EU has noted, however, that non-legal rules such as industry association guidelines are relevant to the "adequacy" determination only to the extent they are complied with and that compliance levels, in turn, are directly related to the availability of sanctions and/or external verification of compliance. *See* European Commission, Directorate General XV, *Working Document: Judging Industry Self-Regulation: When Does it Make a Meaningful Contribution to the Level of Data Protection in a Third Country?* (1998) available at http://www.europa.eu.int/comm/dg15/en/media/dataprot/wp7.htm [hereinafter "*Judging Industry Self-Regulation*"].

54. *Discussion Draft: Elements of Effective Self-Regulation for Protection of Privacy* (1998) available at http://www.ecommerce.gov/staff.htm [hereinafter "*Elements of Effective Self-Regulation*"] (identifying consumer recourse, verification, and consequences as elements of an effective self-regulatory regime).

55. *Id*. Commission staff recently responded to a request from the Direct Marketing Association ("DMA") for an advisory opinion concerning whether the antitrust laws would permit it to require three things of its members: (1) to use the DMA's Mail Preference and Telephone Preference Services to honor consumers' requests to not be contacted by direct marketers; (2) to disclose to consumers how members sell or otherwise transfer personal information about those consumers to others; and (3) to honor consumers' requests that the members not sell or transfer their personal information. FTC Bureau of Competition staff advised the DMA of its conclusion that these requirements, as the DMA described them, would not harm competition or violate the FTC Act. Letter from Bureau of Competition Assistant Director to Counsel for the DMA, Sept. 9, 1997, available at http://www.ftc.gov/os/9710/dma.htm.

56. *See Elements of Effective Self-Regulation*.

57. *FTC Report to Congress/Reference Services* at 25-33. It is still too early to assess the success or efficacy of this plan, because its provisions are not mandatory on its signatories until the end of the year.

58. There may, alternatively, be a role for mechanisms to address practices affecting consumers as a group, such as industry or trade association ethics or screening committees that can resolve broader disputes.

59. *See Elements of Effective Self-Regulation*.

60. Several fair information practice codes suggest compensation for injuries as an important element of fair information practice. *See HEW Report* at 50 (calling for Code of Fair Information Practices that provides for actual, liquidated, and punitive damages); *OECD Guidelines*, Accountability Principle & ¶ 14 and *Explanatory Memorandum* ¶ 62 (accountability supported by legal sanctions); *IITF Report* § III.C ("envision[ing] various forms [of redress] including . . . informal complaint resolution, mediation, arbitration, civil litigation . . . ."); *see also Judging Industry Self-Regulation* at 5.

61. *HEW Report* at 50 (calling for Code of Fair Information Practices that includes civil and criminal penalties, the availability of injunctive relief, and individual rights of action for actual, liquidated, and punitive damages); *OECD Guidelines*, Accountability Principle & ¶ 14 and *Explanatory Memorandum* ¶ 62 (accountability supported by legal sanctions); *IITF Report* § III.C ("envision[ing] various forms [of redress] including . . . informal complaint resolution, mediation, arbitration, civil litigation . . . ."); *EU Directive* arts. 22-23 (judicial remedy and compensation).

62. Two sectoral privacy acts provide for the recovery of actual, liquidated, and punitive damages for violations. *See* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(c) (providing for award of actual damages or liquidated damages of not less than $2,500, punitive damages, attorney's fees, and equitable relief); Cable Communications Policy Act of 1984, 47 U.S.C.

§ 551(f) (providing for recovery of actual damages or liquidated damages of not less than $1,000, punitive damages, and attorney's fees).

63. *HEW* Report at 50; *IITF Report* § III.C (discussing regulatory enforcement and criminal prosecution as redress options); *OECD Guidelines, Explanatory Memorandum* ¶ 62 (referring to accountability supported by legal sanctions); *EU Directive* art. 24 (unspecified sanctions for violations of directive); *see also CSA Model Code* ¶ 4.10.3 (discussing regulatory bodies receiving complaints of violations of fair information practice).

64. *IITF Report* § III.C (redress should be appropriate to violation).

65. The Commission's Deception Policy Statement recognizes that children can be unfairly exploited due to their age and lack of experience. *See* Deception Policy Statement, *appended to Cliffdale Associates, Inc.*, 103 F.T.C. 110, 179 n.30 (1984), *citing Ideal Toy*, 64 F.T.C. 297, 310 (1964). For example, the Commission's actions regarding the marketing of pay-per-call 900 number services to children recognize children as a vulnerable group in the marketplace. *See Audio Communications, Inc.*, 114 F.T.C. 414 (1991) (consent order); *Teleline, Inc.*, 114 F.T.C. 399 (1991) (consent order); *Phone Programs, Inc.*, 115 F.T.C. 977 (1992) (consent order); *Fone Telecommunications, Inc.*, Docket No. C-3432 (June 14, 1993) (consent order). The Telephone Disclosure and Dispute Resolution Act of 1992 prohibits advertising of such services to children under the age of 12, unless the service is a bona fide educational service. 15 U.S.C. §§ 5701 *et seq*.

66. The Federal Educational Rights and Privacy Act of 1974 (FERPA), gives parents of minor students the right to inspect, correct, amend, and control the disclosure of information in education records. 20 U.S.C. § 1232g (1988). The Department of Health and Human Services Policy for Protection of Human Research requires parental/guardian written consent for all DHHS-funded research that involves children as subjects. 45 C.F.R. §§ 46.401-46.409 (1995). The Telephone Disclosure and Dispute Resolution Act of 1992 expressly prohibits advertising of pay-per-call (*e.g.*, 900) services, except bona fide educational services, to children under 12. 15 U.S.C. §§ 5701 *et seq*. (Supp. IV 1992). The Children's Television Act of 1990, among other things, requires television stations and cable operators to limit the amount of advertising during children's television programming. 47 U.S.C. § 303a(b) (Supp. V 1994).

67. *See* Letter from Jodie Bernstein, Director, Bureau of Consumer Protection, Federal Trade Commission, to Center for Media Education, July 15, 1997, available at http://www.ftc.gov/os/9707/cenmed.htm [hereinafter "staff opinion letter"]. Commissioner Azcuenaga did not endorse all of the analyses and conclusions in the staff opinion letter.

68. Providing notice to parents raises some implementation issues, but where the child and parent have separate e-mail addresses, notice could be provided to the parent by e-mail.

69. Mechanisms for obtaining actual or verifiable parental consent include having the parent: mail or fax a signed form downloaded from the site; provide a credit card number; or provide an electronic (digital) signature. An e-mail message submitted without a digital signature may not be adequate to assure parental consent, since a site operator has no means of knowing whether the message is from a parent or a child. This is particularly true because most children do not currently have their own e-mail addresses and instead share their parents' e-mail addresses. While electronic signatures may be the best solution in the future, they may not be widely available at this point. In the meantime, children's Web sites may need to adopt traditional consent mechanisms, such as written consent forms and credit card numbers.

70. It is safe to assume that simply posting a privacy policy at a Web site or advising the child to seek parental permission before providing information online will have little impact on children. Many children will simply ignore these statements. Many will lack the sophistication or judgment to understand a privacy notice or to refrain from providing the requested information. Many children will be unwilling to wait for parental consent, and will provide whatever information is necessary to participate in the site's activity.

71. *See supra* Section III.A.1.

72. 63 Fed. Reg. 10,916 (1998).

73. The following trade associations and industry groups filed guidelines and/or principles: The Bankers Roundtable, Banking Industry Technology Secretariat ("BITS"); Direct Marketing Association ("DMA"); Electronic Messaging Association ("EMA"); Independent Bankers Association of America ("IBAA"); Individual Reference Services Group ("IRSG"); Interactive Services Association ("ISA"); Magazine Publishers of America ("MPA"); National Association of Federal Credit Unions ("NAFCU"); and Smart Card Forum ("SCF"). The Council of Better Business Bureaus, Inc.'s Children's Advertising Review Unit ("CARU") and the DMA also submitted guidelines addressing marketing to children, which are discussed in Section IV.B *infra*.

Numerous individual companies also filed their own privacy policies. Several other organizations and individuals also filed comments in response to the notice. Those filings, which are available for review on the Commission's Web site at http://www.ftc.gov, are not analyzed herein. The Commission's purpose in soliciting *trade association* and *industry group* guidelines was to assess industry's progress towards achieving a self-regulatory regime with respect to information collection online. While the Commission encourages individual companies to adopt information practice policies for the online environment, appreciates all of the submissions it has received in response to the Notice, and commends those firms that have developed effective self-regulatory policies, such policies, as well as the comments of other interested parties, do not constitute the elements of a self-regulatory system, which was the focus of the *Federal Register* Notice.

74. *See, e.g.*, NAFCU cover letter ("NAFCU does recommend that its members post privacy policies on their Web sites").

75. *See* ISA, *Principles on Notice and Choice Procedures for Online Information Collection and Distribution by Online Operators*; DMA, *Marketing Online: Privacy Principles and Guidance*. The DMA encourages members to provide notice of, and substantive choice with respect to, internal secondary uses of information as well (*i.e.*, marketing back by the information collector).

76. The NAFCU submission is the only one that does not address choice.

77. *See* DMA, *Marketing Online: Privacy Principles and Guidance*; MPA submission.

78. *See* ISA, *Principles on Notice and Choice Procedures for Online Information Collection and Distribution by Online Operators*.

79. *See* BITS and IBAA, *Privacy Principles* (BITS and IBAA each submitted the banking industry's *Privacy Principles* independently); SCF, *Consumer Privacy and Smart Cards—A Challenge and an Opportunity*; IRSG, *Individual Reference Services Industry Principles*.

80. *See generally* BITS and IBAA, *Privacy Principles*; NAFCU, *Recommended Privacy Policy*; SCF, *Consumer Privacy and Smart Cards—A Challenge and an Opportunity*; IRSG, *Individual Reference Services Industry Principles*.

81. *See* IRSG, *Individual Reference Services Industry Principles*; DMA, *The Committee on Ethical Business Practice Procedures for Case Handling*.

82. *See* IRSG, *Individual Reference Services Industry Principles*. The IRSG *Principles*, which constitute one model for self-regulation, require independent annual third-party audits, the results of which are made public, and limit the sharing of information with entities that do not adhere to the *Principles*. The DMA has also announced that, effective July 1999, adherence to certain fair information practices (notice and opt-out) will be mandatory for all members. *See* DMA Ethics and Consumer Affairs Department, *Case Report from the Direct Marketing Association's Committee on Ethical Business Practice* (Sept.-Nov. 1997) at 4.

83. The DMA Committee on Ethical Business Practice investigates complaints against companies alleged to be violating DMA's voluntary guidelines. In cases in which a satisfactory resolution of a complaint is not reached, the name of the company and the facts of the case are made public. In addition, the Committee may refer cases to law enforcement agencies and/or to the DMA's Board of Directors for further action including censure, suspension and/or expulsion of a member. This peer review process is non-binding. DMA, *The Committee on Ethical Business Practice Procedures for Case Handling*.

84. Both BITS and IBAA submitted BITS's *Privacy Principles Implementation Plan*. The BITS plan states that establishment of a privacy mark may be necessary, calls upon banks to "apply their own internal process to assure compliance with the bank's privacy principles," and states that "[b]reaches of policy will be addressed internally on a case-by-case basis by each bank." This non-binding reference to ensuring compliance with policies is the only reference to enforcement in any of the submitted guidelines, other than the IRSG *Principles* and the DMA Committee on Ethical Business Practice discussed above.

85. CARU was established by the advertising community as an independent manager of the industry's self-regulatory programs in 1974. Its main activity is the review and evaluation of child-directed advertising in all media. Its Board of Directors consists of representatives from the Council of Better Business Bureaus, the American Association of Advertising Agencies, the American Advertising Federation, and the Association of National Advertisers. CARU is funded directly by members of the children's advertising industry. The DMA represents more than 3,600 member companies interested in database marketing. Its members include catalogers, financial services, publishers, book and music clubs, retail stores, industrial manufacturers, and service industries. Copies of both CARU's and DMA's guidelines are found in Appendix E.

86. The *CARU Guidelines* address children under age 12, while the *DMA Children's Guidelines* do not provide a definition for the term "children."

87. *CARU Guidelines* at 1, 3. The *CARU Guidelines* do not define "passive tracking." However, the term refers to information collected by using navigational software designed to reveal information about the visitor's experience on the site, such as the pages visited, the information downloaded, the content viewed, the operating system used, and the referring site's Internet address.

88. *Id.* at 4.

89. *Id.*

90. *Id.*

91. *Id.*

92. CARU is one of the few trade groups that implements a voluntary enforcement mechanism for both its online privacy guidelines as well as its general media guidelines. In addition to its own monitoring of advertisers, CARU initiates investigations upon receipt of a complaint from a consumer or a company. CARU then seeks the advertiser's compliance with its guidelines and publishes its case reports. If a company is uncooperative and the practices are allegedly deceptive or unfair, CARU refers the matter to the Commission. CARU's voluntary enforcement

mechanism is modeled on that of the National Advertising Division (NAD), which is also associated with the Council of Better Business Bureaus, Inc.

93. Since CARU's founding in 1974, 98% of the subjects of its investigations have complied with its decisions.

94. The *CARU Guidelines* apply generally to marketers of children's products and services. Since CARU is not a membership organization, however, adherence to its guidelines is not mandatory. Each of CARU's leading organizational sponsors has urged its own members to implement the *CARU Guidelines*, but these sponsors do not make adherence mandatory for their members.

95. The *DMA Children's Guideline*s suggest that marketers use language such as "Your mom or dad should say it's okay for you to answer these questions," but are not explicit with respect to when parental permission should be sought. *DMA Children's Guidelines*, Guideline No. 1.

96. *DMA Children's Guidelines*, Guideline Nos. 1-2.

97. McCain/Bliley letters. Specifically, the Commission stated that "[w]e hope to find by March 1, 1998, that a substantial majority of commercial Web sites are clearly posting their information practices and privacy policies." *Id*. at n.2.

98. The samples for groups A-D were drawn from a comprehensive list of commercial Web sites provided by the Dun and Bradstreet Corporation. *See* Appendix A.

99. The terms "likely to be of interest to consumers" and "primarily directed to children aged fifteen or younger" are defined in Appendix A.

100. For a copy of the Survey Forms used by the surfers, see Appendix C.

101. These figures are based on data supplied by The Dun & Bradstreet Corporation. Figures do not total 100%. Approximately 3% of the sites in all the samples are not classified by size, because sales figures were unavailable. For a description of the Dun & Bradstreet database used in this survey, see Appendix A.

102. *See* Appendix D, Table 1.

103. *See* Appendix D, Table 1.

104. *See* Appendix D, Table 1.

105. Company size information was not obtained for Web sites in this sample.

106. *See supra* Section II.B.

107. The rates are: 92% of the sites in the Comprehensive Sample; 88% of the Health Sample sites; 87% of the Retail Sample sites; 97% of the Financial Sample sites; and 97% of the Most Popular Sample sites. *See* Appendix D, Table 3, which also sets forth statistics based upon company size.

108. For purposes of this survey, the provision of a mechanism for sending e-mail to a site's Webmaster, without more, was not considered collection of an e-mail address. A site's invitation to online consumers to "Contact Us" or "Send Us Your Comments" by e-mail, however, was deemed to be collection of an e-mail address. When the collection of an e-mail address is not considered, the number of sites collecting personal information decreases slightly in all samples. Thus, 65% of all sites in the Comprehensive Sample collect some personal information other than an e-mail address; as do 53% of the sites in the Health Sample; 67% of the sites in the Retail Sample; 73% of the sites in the Financial Sample; and 94% of the sites in the Most Popular Sample. *See also infra* note 115. Because the survey form did not identify the manner of e-mail collection, the above statistics exclude *all* sites that collect only an e-mail address, including those sites that ask for it in contexts other than "Contact Us," such as on registration forms, etc.

109. For similar information with respect to the other samples, see Appendix D, Table 5.

110. *See* Appendix D, Table 4.

111. *Id*.

112. The Commission cannot report on the number of companies in the survey that create such profiles, because the survey concerns Web sites' disclosures, and not actual practices.

113. The numbers for the Health, Retail and Financial samples are as follows: sites collecting five or more additional types of information — 12% (Health), 19% (Retail), 26% (Financial); sites collecting three or more additional types of information — 36% (Health), 60% (Retail), 53% (Financial); sites collecting at least one additional type of information — 57% (Health), 76% (Retail), 73% (Financial). *See* Appendix D, Table 6.

114. *See* Appendix D, Table 2.

115. *See* Appendix D, Table 7. The percentage of disclosures among sites that collect some personal information other than an e-mail address is slightly higher: 21% in the Comprehensive Sample; 24% in the Health Sample; 18% in the Retail Sample; 22% in the Financial Sample; and 74% in the Most Popular Sample. *See also supra* note 108.

116. *See* Appendix D, Table 8.

117. *See* Appendix D, Table 9.

118. *See* Appendix D, Table 2.

119. *See* Appendix D, Table 7.

120. *See* Appendix D, Table 8.

121. *See* Appendix D, Table 9. Some sites post both a Privacy Policy Notice and one or more Information Practice Statements.

122. *See, e.g.*, Communications Daily (Untitled, February 10, 1998); Washington Telecom Newswire (Untitled, February 9, 1998); I. Teinowitz, "*FTC Will Survey Marketer Web Sites for Privacy*," Advertising Age (February 1998), available at http://www.adage.com/interactive/articles/19980216/article1.html.

123. *See* Appendix D, Table 7.

124. Given the small number of sites involved, statistics based upon company size have not been reported.

125. The rate is 33% (or 31 sites) for the Comprehensive Sample, 32% (or 6 sites) for the Health Sample, 33% (or 6 sites) for the Retail Sample, and 35% (or 7 sites) for the Financial Sample. *See* Appendix D, Table 10. In responding to the relevant question on the General Survey Form, staff counted both statements giving choice regarding internal uses of the personal information and statements giving choice about the transfer of the information to third parties as statements offering consumers choice about how the information collected will be used. *See* Appendix C.

126. The rate is 10% (or 9 sites) for the Comprehensive Sample. *See* Appendix D, Table 10.

127. The rate is 6% (or 1 site) for the Retail Sample and 5% (or 1 site) for the Financial Sample. *See* Appendix D, Table 10.

128. *See* Appendix D, Table 11. The rate for the Health Sample is 32% (or 6 sites) and the rate for the Retail Sample is 22% (or 4 sites). Statements such as "We keep this information confidential" were counted as assertions of non-disclosure to third parties.

129. *See* Appendix D, Table 11. Statements indicating that demographic or interest information may be shared with third parties were counted as assertions of possible third-party disclosures.

130. *See* Appendix D, Table 12. When expressed as a percentage of *all* sites in a given sample (and not just those sites that collect personal information and have an information practice disclosure), the percent of sites offering choice, access, or security, or addressing disclosures to third parties, is even lower. Thus, only 5% of all sites in the Comprehensive Sample, 4% of all sites in the Health and Retail Samples, and 6% of all sites in the Financial Sample state that they

offer consumers choice; 1% of all sites in the Comprehensive Sample, 2% of all sites in the Retail Sample and no sites in the Health and Financial Samples state that they offer consumers access; 2% of all sites in the Comprehensive Sample, no sites in the Health Sample, and 1% of all sites in the Retail and Financial Samples state that they take data security measures; 5% of all sites in the Comprehensive Sample, 4% of all sites in the Health Sample, and 3% of all sites in the Retail and Financial Samples state that they will not disclose any personal information collected to third parties; and 5% of all sites in the Comprehensive Sample, 4% of all sites in the Health and Retail Samples, and 6% of all sites in the Financial Sample state that they may disclose some or all of the personal information collected to third parties.

131. *See* Appendix D, Table 10.

132. *Id.*

133. *Id.*

134. *See* Appendix D, Table 11.

135. *Id.* Again, the above figures are significantly lower when expressed as a percentage of *all* sites in the Most Popular Sample. Thus, 49% of all sites in the Most Popular Sample state that they offer consumers choice; 27% state that they offer consumers access; 12% state that they take data security measures; 10% state that none of the personal information collected will be disclosed to third parties; and 56% state that some or all of the personal information collected may be disclosed to third parties.

136. *See* Appendix D, Table 12.

137. *See* Appendix D, Table 3.

138. *See* Appendix D, Table 13.

139. As in the General Survey, a mere hyperlink to a site's Webmaster was not considered collection of an e-mail address for purposes of this survey. However, hypertext that asks visitors to "Contact Us" or "Send Us Your Comments" was included as collection of an e-mail address. *See supra* note 108.

140. *See* Appendix D, Table 5.

141. *See* Appendix D, Table 6.

142. For instance, in order to register for certain online activities, some sites require children to identify their interests such as rollerblading, skateboarding, ice skating, biking, video games, science, football, soccer, and computer games. Other sites ask children information about their

favorite television shows, commercials, and musical groups.

143. For example, one site asks children personal financial questions such as the following:

> Do you own mutual funds?
> Are your parents currently saving for your college education?
> What do you usually do with gifts of money?

144. *See* Appendix D, Table 2. The higher disclosure rate for the Children's Sample may reflect the fact that staff publicly disclosed that this sample would be selected from sites listed in the Yahooligans! Directory.

145. *Id.*

146. *See* Appendix D, Table 9.

147. *See* Appendix D, Table 8.

148. *See* Appendix D, Table 10.

149. *Id.*

150. *Id.*

151. *Westin Survey* at 3.

152. *See* Appendix D, Table 13.

153. *See* Appendix D, Table 11.

154. *Id.*

155. *See* Appendix D, Table 13.

156. *Id.*

157. *Id.*

158. *Id.* Examples of opt-out statements include: "When minors subscribe to the newsletter, they are asked for their parent's e-mail informing them [sic] their kid has subscribed to the e-mail and the parent has the option to discontinue this subscription," and "All parents can correct or remove any information we receive from a child by contacting us online, by phone or mail."

159. *Westin Survey* at 3.

160. Current American privacy law can best be described as sectoral, consisting of a handful of disparate statutes directed at specific industries that collect personal data and none of which specifically covers the collection of personal information online. *See, e.g.*, Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681 *et seq*. (governing consumer credit reports); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510 *et seq*. (governing electronic mail and voicemail communications); Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (governing cable television subscriber information); Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401 *et seq*. (governing individual bank records); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (governing video rental records); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (governing student records); Communications Act of 1934, *as amended by*, Telecommunications Act of 1996, 47 U.S.C. § 222 (governing information relating to use of telecommunication services ["customer proprietary network information"]); *cf*. Privacy Act of 1974, 5 U.S.C. § 552a (governing data collected by the federal government). Pursuant to the Supreme Court's decision in *United States v. Miller*, 425 U.S. 435 (1976), individuals have no Fourth Amendment interest in personal information they voluntarily have conveyed to another. Consequently, any privacy protections for personal information must be legislatively grounded.

161. 15 U.S.C. §§ 41 *et seq*.

162. *See supra* note 67.

163. Parental notice raises some implementation issues. In those instances where parents and children have separate e-mail addresses, notice may be provided to parents electronically. Where verifiable parental consent is required, sites can simply direct children to download (print) the notice and consent form and have the parent return the signed form by regular mail or facsimile.

APPENDIX A: METHODOLOGY

APPENDIX B: SURFER INSTRUCTIONS (GENERAL AND CHILDREN'S SURVEYS)

APPENDIX C: SURVEY SAMPLES AND RESULTS

APPENDIX D: SUPPORTING DATA TABLES

APPENDIX E: INDUSTRY GUIDELINES

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

LabMD, INC., Plaintiff, v. FEDERAL TRADE COMMISSION, Defendant.	Civil Action No.: _____ *Related Case*: FTC v. LabMD et al., 1:12-cv-3005-WSD

VERIFIED COMPLAINT
FOR DECLARATORY AND INJUNCTIVE RELIEF

Plaintiff LabMD, INC. ("LabMD") hereby states its complaint for declaratory and injunctive relief against the unconstitutional abuse of government power and ultra vires actions by Defendant Federal Trade Commission (the "FTC" or "Commission") as follows:

PARTIES, JURISDICTION, AND VENUE

1. LabMD, 1250 Parkwood Circle, Unit 2201, Atlanta, GA 30339, is a small medical cancer diagnostics business.

2. The FTC, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580, is a federal agency for purposes of the Administrative Procedure Act ("APA"), 5 U.S.C. § 551 et seq.

3. This Court has subject-matter jurisdiction under 28 U.S.C. § 1331, 28 U.S.C. § 2201, and 5 U.S.C. § 702. In LabMD v. FTC, Case No. 13-15267-F, at 2 (11th Cir. Feb. 18, 2014), the United States Court of Appeals for the Eleventh Circuit examined whether it had jurisdiction to entertain LabMD's claims against the FTC under the APA, as codified in relevant part at 5 U.S.C. §§ 701-06, under the federal Constitution, and under 28 U.S.C. § 1331, which allows for "nonstatutory" review of ultra vires agency actions. The Court held:

> [J]urisdiction to hear suits under the APA is conferred by 28 U.S.C. § 1331, which provides district courts original jurisdiction of all civil actions arising under the laws of the United States. Any APA, *ultra vires*, and constitutional claims, to the extent they can be asserted [by LabMD] at this stage, first must be asserted and considered in a district court.

(internal citations omitted). A true and correct copy of the foregoing Order is attached hereto as Exhibit 1 and is incorporated herein by reference. See also Sackett v. E.P.A., 132 S. Ct. 1367, 1373 (2012) (". . . the APA provides for judicial review of all *final* agency actions . . . ."); id. at 1374 ("The Court holds that the Sacketts may immediately litigate their jurisdictional challenge in federal court. I agree, for the Agency has ruled definitively on that question.") (Ginsburg, J. concurring). The grounds for the relief requested include the due process clause of the United States Constitution, 5 U.S.C. §§ 701-706 (APA's judicial review provisions), 28 U.S.C. §

1651 (the All Writs Act), 28 U.S.C. § 2201 (the Declaratory Judgment Act), and 28 U.S.C. § 2202 (further relief).

4. The FTC has finally determined that it has jurisdiction over LabMD and that it has complied with constitutional due process fair-notice requirements: In the Matter of LabMD, Inc., FTC Dkt. No. 9357 (Jan. 16, 2014). A true and correct copy of the foregoing order is attached hereto as Exhibit 2 and is incorporated herein by reference.

5. The FTC claims the foregoing decision marks the consummation of its decisionmaking process, has the force of law, and is entitled to deference under "Chevron." See Supplemental Letter Brief, FTC v. Wyndham Worldwide Corp. et al., Case No. 2:13-cv-01887-ES-JAD, Dkt. 152-1, at 6 (Jan. 21, 2014). A true and correct copy of the foregoing brief is attached hereto as Exhibit 3 and is incorporated herein by reference.

6. Venue is proper under 28 U.S.C. §1391(e).

NATURE OF THE CASE

7. LabMD, at all relevant times a small medical laboratory providing doctors with cancer-detection services, is now on the verge of ceasing all operations after being trapped in a paralyzing web of government investigations, subpoenas, and administrative litigation.

8. At some unknown point between 2005 and August 2013, the FTC, through enforcement activities and/or internet postings on the FTC's website, rather than through administrative rulemaking, guidance or known standards, declared for the first time that certain unspecified patient-information data-security practices employed by LabMD were inadequate and thus an "unfair" trade practice under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("Section 5").

9. The FTC still has yet to issue any rule or statement with legal force and effect describing the specific patient-information data-security practices it believes Section 5 prohibits or permits.

10. Between 2005 and the present, the FTC never specified in a rule or statement with legal force and effect how LabMD's patient-information practices fell short or described what, exactly, it should have done differently at any given point. In fact, the FTC commenced an investigation of LabMD in January 2010, filed its administrative complaint in August 2013, and still today, LabMD has yet to be told what, exactly, it did wrong at any point during the relevant period of years.

11. The FTC's actions and a campaign of disparagement, including conclusory statements by an FTC Commissioner that LabMD had mishandled sensitive patient information made shortly after the administrative complaint had been filed, have eviscerated LabMD's business and destroyed its professional reputation.

12. In October, 2013, LabMD lost its directors and officers (D&O) liability insurance as a result of the pending enforcement action and has been unable to obtain D&O insurance because of the pending action.

13. Further, LabMD and its doctors were denied "tail" medical malpractice insurance because of the FTC's actions, which will, unless this matter is resolved favorably in the near future, severely limit LabMD's prospects for obtaining medical malpractice insurance going forward and thus hiring qualified physicians.

14. The company's insurance carrier has advised that it will not renew LabMD's general liability insurance policy effective May 6, 2014, so that the policy will terminate effective October, 2014. This means that LabMD cannot rent office space.

15. The FTC's actions have forced LabMD, a company that once employed more than forty people and provided diagnostic services to more than one hundred doctors, to stop accepting samples.

16. At all times relevant, LabMD's Protected Health Information ("PHI"), or patient-information, data-security practices were subject to comprehensive regulation by the U.S. Department of Health and Human Services ("HHS") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 U.S.C. § 1320d et seq., and the Health Information Technology for Economic and Clinical Health Act

("HITECH"), 42 U.S.C. §§ 300jj et seq., 17901 et seq. See http://www.healthit.gov/providers-professionals/ehr-privacy-security/practice-integration .

17. Neither the HHS nor the FTC has accused LabMD of violating HIPAA or HITECH. See Complaint, In the Matter of LabMD, Inc., FTC Dkt. No. 9357 (Aug. 28, 2013). A true and correct copy of the foregoing complaint is attached hereto as Exhibit 4.

18. Even if Section 5 does empower the FTC to broadly regulate data-security, which it does not, Congress delegated sole authority to regulate PHI data-security to the HHS. And even if Section 5 does empower the FTC to regulate PHI data-security concurrently with HHS and/or to "overfile" HHS using a "common law" of consent orders and internet posts to impose requirements in excess of those set through HHS rulemaking, which it does not, the Commission's refusal to promulgate rules or regulations and provide the public with proper notice and comment violates LabMD's due process rights by failing to give fair notice of what the FTC believes Section 5 forbids or requires.

19. Not only does the FTC lack the statutory authority to regulate PHI and/or cyber-security, it also lacks the expertise to do so. For example, Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," 78 Fed. Reg. 11739 (Feb.

19, 2013), available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (accessed Mar. 18, 2014), directed the Department of Commerce to set data-security standards, not the FTC.

20. To stop the abuse, LabMD seeks a declaration that the FTC lacks jurisdiction under Section 5 over PHI data-security practices and that the FTC has violated LabMD's due process and First Amendment rights. It also seeks preliminary and permanent injunctive relief staying the administrative proceedings in In the Matter of LabMD, Inc., FTC Dkt. No. 9357. Finally, LabMD asks that the FTC pay all of LabMD's attorneys' fees and litigation costs.

FACTS

21. Section 5 authorizes the FTC to prohibit "unfair or deceptive acts or practices in or affecting commerce."

22. The FTC in this case claims Section 5 "unfairness" authority to regulate LabMD's PHI data-security practices, even absent a claim of "deception," by way of administrative "common law" established through consent orders and Internet postings.

I. The FTC Targets LabMD.

23. In or about 2008, Tiversa Holding Corp. ("Tiversa"), a self-described "cyber-intelligence company" specializing in searching for and copying medical,

financial, and other sensitive files on peer-to-peer networks using patented technology, obtained a LabMD accounts-receivable computer file containing PHI without LabMD's knowledge or consent.

24. On May 13, 2008, Tiversa contacted LabMD, advised it that Tiversa had taken its property, and refused to provide information on the procurement of the file unless LabMD entered into a contract for Internet security services. LabMD turned down this offer. See Dissenting Statement of Commissioner J. Thomas Rosch, Petitions of LabMD, Inc. and Michael J. Daugherty to Limit or Quash the Civil Investigative Demands, FTC File No. 1023099 (June 21, 2012). A true and correct copy of the foregoing dissent is attached hereto as Exhibit 5 and is incorporated herein by reference.

25. In 2009, Tiversa gave LabMD's PHI accounts-receivable file to the FTC under highly irregular circumstances. See id. Recent deposition testimony of Tiversa's CEO, Robert Boback, suggests the FTC and Tiversa met on multiple occasions and ultimately conspired and agreed to transfer LabMD's file via a FTC civil investigative demand (CID) to a third company (the "Privacy Institute") that, upon information and belief, is a company that has a relationship with a Tiversa advisory board member.

26. Beginning in January 2010, the FTC requested and LabMD voluntarily provided thousands of pages of documents and submitted to multiple meetings and interviews.

27. Then, on December 21, 2011, the FTC issued formal civil investigative demands (the "CIDs") to LabMD.

28. LabMD filed a Petition to Limit or Quash the CIDs on January 10, 2012, explaining, among other things, that LabMD's PHI data security was exclusively regulated by HHS and solely subject to HHS rules and regulations establishing data-security standards for PHI under HIPAA and HITECH.

29. Commissioner Julie Brill denied LabMD's petition on April 20, 2012. Commission Letter Denying LabMD, Inc.'s Petition to Limit or Quash the Civil Investigative Demand and Michael J. Daugherty's Petition to Limit or Quash the Civil Investigative Demand, in File No. 1023099, at 13 (April 20, 2012). A true and correct copy of the foregoing correspondence is attached hereto as Exhibit 6 and is incorporated herein by reference.

30. Commissioner Brill acknowledged that LabMD's PHI accounts-receivable spreadsheet file "can be considered" protected health information regulated under HIPAA and HITECH but claimed that the FTC jurisdiction under Section 5 was "overlapping and concurrent." Id.

31. On April 25, 2012, LabMD appealed Commissioner Brill's ruling, arguing, as the Commission recently admitted, that the FTC "does not enforce HIPAA or HITECH." See Ex. 2 at 12 & n.19. LabMD also challenged the FTC's reliance on the PHI accounts-receivable file obtained from Tiversa.

32. Nonetheless, on June 21, 2012, three Commissioners (including Commissioner Brill) affirmed Commission Brill's ruling, "finding its conclusions to be valid and correct." See Commission Letter Affirming the Ruling, By Commissioner Brill, Denying the Petitions To Limit or Quash Filed by LabMD and Michael J. Daugherty (June 21, 2012). A true and correct copy of the foregoing order is attached hereto as Exhibit 7 and is incorporated herein by reference. Then-Commissioner Thomas Rosch dissented. Ex. 5.

33. The FTC then filed a petition to enforce the CIDs in this Court. LabMD opposed the petition, arguing, among other things, that the FTC lacked jurisdiction to regulate data-security.

34. The Hon. William S. Duffey upheld the CIDs, but said "there is significant merit" to LabMD's argument that Section 5 does not justify an investigation into data-security practices and consumer privacy issues. See Opinion and Order, FTC v. LabMD et al., 1:12-cv-3005-WSD, Dkt. No. 23, at 4 (N.D. Ga.

Nov. 26, 2012) (Duffy, J.). A true and correct copy of the foregoing order is attached hereto as Exhibit 8.

II. LabMD Publicly Criticizes The FTC And The FTC Retaliates.

35. LabMD's owner, Michael Daugherty decided to warn the public about the FTC's abuses through the press, social media, and a book. Mr. Daugherty used, and continues to use, his website, http://michaeljdaugherty.com/, to criticize the government.

36. For example, Mr. Daugherty was quoted in a September 7, 2012, Atlanta Business Chronicle article as follows: "'We are guilty until proven innocent with these people . . . . They are on a fishing expedition. We feel like they are beating up on small business.'" Amy Wenk, "Atlanta Medical Lab Facing Off Against FTC," Atlanta Business Chronicle (September 5, 2012). Ms. Wenk wrote that "Daugherty contends his company is being unreasonably persecuted by FTC. He said he's already spent about $500,000 fighting the investigation." Id.

37. On information and belief, FTC attorney Alain Sheer, who would later serve as lead counsel for the FTC in an enforcement action against Plaintiff, monitored Mr. Daugherty's political speech and retaliated against him for it.

38. For example, on July 19, 2013, Mr. Daugherty posted the trailer to his book, "The Devil Inside the Beltway," on his website,

http://michaeljdaugherty.com/2013/07/19/the-devil-inside-the-beltway-book-trailer/. The trailer called the FTC's actions against LabMD an "abusive government shakedown" and explained that his book would "blow the whistle" about how "the Federal Trade Commission began overwhelming . . . [LabMD, a] small business, a cancer detection center, with their abusive beltway tactics." It criticized Commission staff, including Mr. Sheer.

39. On July 22, 2013, Mr. Sheer told LabMD that Commission staff had recommended that the FTC commence enforcement proceedings against LabMD.

40. On July 30, 2013, Janis Claire Kestenbaum, the Senior Legal Advisor to the Chairwoman of the FTC, provided LabMD a draft complaint.

41. On August 28, 2013, the Commission commenced an enforcement action (the "Enforcement Action") by issuing a complaint and notice order. The gravamen of its claim at that time was about the PHI accounts-receivable file purloined by Tiversa. Mr. Sheer, who met with Tiversa and who was responsible for the shell-game through which the FTC obtained the file, is lead Complaint Counsel.

42. The FTC's Complaint in the Enforcement Action makes clear that LabMD was a "health care provider" and subject to HIPAA, which comprehensively regulates patient-information data-security, among other things.

43. The FTC did not allege that LabMD violated PHI data-security standards and breach-notification requirements established by HIPAA and HITECH and HHS regulations implementing those statutes.

44. Instead, the FTC's Complaint solely alleged that LabMD violated Section 5's proscription against "unfair" trade practices. It said LabMD's "information security program" was not "comprehensive" and that LabMD did not use "readily available measures" or "adequate measures" but did not specify what those terms actually mean. See Ex. 4 ¶¶ 10-11.

45. The FTC did not name an individual complainant or allege direct harm to any person.

46. The FTC did not cite any regulations, guidance, or standards for what was "adequate," "readily available," "reasonably foreseeable," "commonly known," or "relatively low cost."

47. The FTC did not cite any regulations, guidance, or standards that LabMD supposedly failed to comply with, or specify the combination of LabMD's alleged failures to meet the unspecified regulations, guidance, or standards that, "taken together," allegedly violated Section 5.

48. The FTC did not allege that LabMD's data-security practices fell short of meeting medical-industry data-security standards, such as those established by HIPAA and HITECH for PHI data security.

49. Mr. Sheer of the FTC has admitted that "[n]either the complaint nor the notice order prescribes specific security practices that LabMD should implement going forward." Initial Pretrial Conference Transcript, In the Matter of LabMD, Inc., Dkt. No. 9357, 10:11-15 (Sept. 25, 2013) ("Initial Pretrial Conf. Trans."). He also acknowledged that the FTC brought this action without any complaining witnesses who say their data was released or disclosed. Id. 33:3-5. A true and correct copy of that transcript is attached hereto as Exhibit 9.

50. No court has ever held the FTC may require firms to adopt information-practice policies under Section 5's "unfairness" prong. Hearing Trans. 16: 22-25, FTC v. LabMD, Inc. et al., Case No. 1:12-cv-3005-WSD (Sept. 19, 2012) (Duffy, J.) (emphasis added). A true and correct copy is attached hereto as Exhibit 10.

51. On September 17, 2013, LabMD filed an answer challenging the FTC's jurisdiction and violations of LabMD's federal constitutional due process rights, among other things.

52. In September 2013, HHS said that it decided against even investigating LabMD's alleged PHI data-security practices, noting that it had not received any complaints.

53. On October 24, 2013, Mr. Sheer of the FTC served a subpoena duces tecum on Mr. Daugherty, LabMD's CEO and President, requesting the following documents concerning Mr. Daugherty's book:

- "All drafts of . . . [Mr. Daugherty's book about the FTC] that were reviewed by any third party prior to the Manuscript's publication."
- "All comments received on drafts of" Mr. Daugherty's book about the FTC.
- "All documents related to the source material for drafts of" Mr. Daugherty's book about the FTC, "including documents referenced or quoted in the" book.
- "All promotional materials related to" Mr. Daugherty's book criticizing the FTC, "including, but not limited to, documents posted on social media, commercials featuring . . . [Mr. Daugherty], and presentations or interviews given by" Mr. Daugherty.

54. After over four years of investigation and litigation, LabMD still does not know when or what it did "wrong" and cannot even determine what the elements of a data-security "unfairness" offense are in this case.

55. For example, FTC enforcement staff have refused to substantively respond to LabMD's interrogatories regarding PHI data-security standards—including "data-security standards, regulations, and guidelines the FTC seeks to enforce against LabMD"—except to cross-reference their response to LabMD's request that they produce "[a]ll documents sufficient to show the standards or criteria the FTC used in the past and is currently using to determine whether an entity's data-security practices violate Section 5 of the Federal Trade Commission Act from 2005 to the present."

56. Indeed, Complaint Counsel even objected to LabMD's interrogatory inquiring what "data-security standards, regulations, and guidelines the FTC will use to determine whether LabMD's data-security practices were not reasonable and appropriate" on the ground that it seeks opinions by undisclosed nontestifying experts and "calls for expert opinions."

57. The thousands of pages of materials that FTC enforcement staff have produced to LabMD in response to the foregoing document request (most of which was produced on March 3, 2014, two days before the close of fact discovery) consist almost exclusively of: Power Point presentations; FTC staff reports; emails; FTC Consumer Alerts, OnGuard posts, Guides for Business, FTC Office of Public Affairs blog posts, and assorted other Internet postings; materials FTC staff employees apparently use to prepare for presentations, including handwritten notes; copies of

FTC administrative complaints, draft administrative complaints, consent orders, and related documents; letters the FTC has sent to various companies; documents related to various FTC workshops; speeches given by various FTC Commissioners; assorted congressional testimony; and other miscellaneous materials. Some of these materials are of very recent vintage and dated after the events described in the FTC's August 2013 administrative complaint allegedly occurred. Some of these materials are dated after August 28, 2013, when the FTC issued this complaint. The only regulations that FTC enforcement staff produced to LabMD do not apply to LabMD and implement statutes that also do not apply to LabMD.

58. On March 3, 2014, FTC enforcement staff refused to admit, among other things, that the FTC's administrative complaint does not specifically reference any industry standards for data-security practices, hardware or software necessary to avoid a violation of Section 5, instead claiming that LabMD was asking for "an admission irrelevant to any permissible claim or defense in this administrative proceeding and outside of the scope of discovery" and, in the alternative, denying that they were required to allege this.

59. FTC enforcement staff have even argued that "STANDARDS USED TO ENFORCE SECTION 5 ARE OUTSIDE THE SCOPE OF DISCOVERY," saying that "[t]he orders and opinions of the Commission and of th[e ALJ] …

preclude such discovery." Complaint Counsel's Motion for Protective Order Regarding Rule 3.33 Notice of Deposition, *In the Matter of LabMD*, FTC Dkt. No. 9357, at 7 (Feb. 14, 2014).

60. More recently, on March 18, 2014, FTC enforcement staff produced an expert witness report that for the first time—after more than four years of investigation and litigation—gave LabMD some notice as to what a FTC expert thinks LabMD did wrong. But that report did not even purport to assess LabMD's PHI data-security practices against any objective, applicable medical-industry data-security statute, regulation, custom, or standard.

III. LabMD Challenges The FTC's Jurisdiction.

61. On November 12, 2013, LabMD filed a dispositive Motion to Dismiss raising pure issues of law and questions of statutory interpretation in the FTC's administrative case. A true and correct copy is attached hereto as Exhibit 11. LabMD requested oral argument. Under the FTC's Rules of Practice, Commissioners (and not the ALJ) rule on dispositive motions to dismiss complaints they recently voted to issue in the first instance.

62. On November 14, 2014, LabMD also filed a Verified Complaint in the U.S. District Court for the District of Columbia seeking solely injunctive and

declaratory relief. LabMD v. FTC et al., Case No. 1:13-cv-01787-CKK, Dkt. No. 1 (D.D.C. Nov. 14, 2013).

63. On November 18, 2013, LabMD filed a petition for review in the U.S. Court of Appeals for the Eleventh Circuit, LabMD, Inc. v. FTC, Case No. 13-14267-F (11th Cir. Nov. 18, 2013). Ex. 1.

64. On November 25, 2013, LabMD filed an administrative stay motion in the FTC enforcement action.

65. On December 2, 2013, LabMD filed a reply in support of its administrative motion to dismiss. A true and correct copy is attached hereto as Exhibit 12.

66. On December 13, 2013, the FTC issued an order denying LabMD's stay motion ("December 13 Order"). A true and correct copy is attached hereto as Exhibit 13. The December 13 Order states that no Article III court has jurisdiction over LabMD's claims until the FTC gives its permission.

67. On December 16, 2013, the Eleventh Circuit issued two jurisdictional questions to the parties. Jurisdictional Questions, LabMD v. FTC, Case No. 13-15267-F (Dec. 16, 2013).

68. On December 23, 2013, LabMD filed a stay motion in in the Eleventh Circuit. Petitioner's Motion for Stay Pending Review, LabMD v. FTC, Case No. 13-15267-F (Dec. 23, 2013).

69. On January 16, 2014, the FTC denied LabMD's administrative Motion to Dismiss, rejecting LabMD's jurisdictional and fair-notice due process challenges without oral argument, thereby denying LabMD an opportunity to create a record (the "January 16 Order"). Ex. 2.

70. On January 17, 2014, the FTC submitted the January 16 Order to the Eleventh Circuit, via what it called a "notice of supplemental authority."

71. FTC did the exact same thing on the exact same day in FTC v. Wyndham Worldwide Corp. et al., Case No. 2:13-cv-01887-ES-SCM, Dkt. No. 151 (D. N.J. Jan. 17, 2014). The FTC claimed its order had the force of law and should be given deference under "Chevron." Ex. 3 at 6.

72. The FTC admits that it cannot and does not enforce HIPAA or HITECH. Ex. 2 at 12 & n.19.

73. The FTC admits that its case against LabMD solely alleges statutory Section 5 statutory "unfairness" violations, not "violations of the FTC's Health Breach Notification Rule." Id. at 20 n.20.

74. The FTC admits that it has failed to establish any data-security standards with the force of law that give notice as to what PHI data-security practices the Commission and its enforcement staff believes Section 5 forbids or requires. Ex. 2 at 15.

75. The FTC admits that it did not claim data-security regulatory authority until years after 1994, when Section 5 was last amended to add subsection (n). 15 U.S.C. § 45(n). Ex. 2 at 4, 8-9. Subsection (n) does not mention "data security," let alone explain what data-security practices the FTC believes Section 5 to forbid or require.

76. Yet the FTC claims subsection (n) gives fair notice: "Here, the three-part statutory standard governing whether an act or practice is 'unfair,' set forth in Section 5(n) [15 U.S.C. § 45], should dispel LabMD's concern about whether the statutory prohibition of 'unfair . . . acts or practices' is sufficient to give fair notice of what conduct is prohibited." Ex. 2 at 16.

77. The FTC's January 16 Order essentially asserts that constitutional fair-notice due process requirements are somehow inapplicable here because, according to the Defendant, the FTC is not pursuing "criminal punishment or civil penalties for past conduct." Ex. 2 at 16.

78. The FTC also claims it is not obligated to provide any fair notice at all of the PHI data-security practices it believes Section 5 to forbid or require because agencies have broad "discretion" to "address an issue by rulemaking or adjudication." Ex. 2 at 15.

79. For that matter, the FTC effectively claims that the standard for Section 5 "unfairness" PHI data-security liability is whether a company's practices are "unreasonable" according to it, while acknowledging that this is a case of first impression as to what is "unreasonable."

80. Elsewhere, the FTC admitted that there is no process through which businesses could have obtained guidance or an advisory opinion from the Commission regarding data-security practices. See Hearing Trans., FTC v. Wyndham et al., Case No. 2:13-cv-01887-ES-SCM, 52:10-11 (Nov. 7, 2012). A true and correct copy of an excerpt of the foregoing transcript is attached hereto as Exhibit 14 and is incorporated herein by reference.

81. On February 18, 2014, the Eleventh Circuit dismissed LabMD's Petition for Review and denied all pending motions as moot because there was no cease and desist order reviewable under 15 U.S.C. § 45(c). Instead, it ruled this Court has original jurisdiction over LabMD's ultra vires, statutory, and constitutional claims to

the extent that such claims could be asserted before a cease and desist order is entered. Ex. 1.

82. Therefore, on February 19, 2014, LabMD filed a Notice of Voluntary Dismissal Without Prejudice of LabMD v. FTC et al., Case No. 1:13-cv-01787-CKK, Dkt. No. 20 (D.D.C.), because under D.C. Circuit law, which is different from the law of this Circuit, only the U.S. Court of Appeals for the D.C. Circuit has jurisdiction over those claims, yet the D.C. Circuit will never have jurisdiction under 15 U.S.C. § 45(c) because LabMD has not done business there.

83. The FTC has issued a final agency decision regarding jurisdiction, and LabMD has exhausted all administrative remedies with respect to its jurisdictional and constitutional fair-notice due process arguments.

IV. The FTC Denies LabMD Procedural Due Process.

84. To begin with, the FTC has never specified the PHI data-security standards LabMD failed to meet, thereby denying LabMD an opportunity to effectively defend itself and granting the Commission, Mr. Sheer, and other federal bureaucrats unlimited discretion to decide what is "unreasonable" after the fact and to regulate the entire health care industry based on their idiosyncratic whim, caprice, and fancy.

85. In 2009, the FTC modified its Rules of Practice to deny respondents a fair defense and to render motion practice futile. 74 Fed. Reg. 20,205 (May 1, 2009).

86. At the initial pretrial conference, the ALJ told LabMD's counsel:

> [L]et me talk about dispositive motions . . . . There is a rule that covers that, if you intend to file a summary judgment, and if you don't know, I'll tell you. Summary judgments will be ruled on by the Commission, the same body that voted to issue the complaint in this case. With respect to motion to dismiss or other substantive motion, the rules provide that if they are filed before the start of the evidentiary hearing, they will be ruled on by that same Commission . . . .

Ex. 9 at 18:11-15. The ALJ lacks power to even grant a continuance of the evidentiary hearing or stay the proceedings pending adjudication of dispositive motions before the Commission. See 16 C.F.R. §§ 3.22(b), 3.41(b).

87. The FTC was extensively warned about the constitutional implications of its power-grab during the comment period.

88. The American Bar Association (ABA) Section of Antitrust Law ("Antitrust Section") said the revisions forced respondents to address prehearing issues to the FTC without the benefit of a prior opinion authored by a party who was not involved in crafting and approving a complaint. Comments of the ABA Section of Antitrust Law in Response to the Federal Trade Commission's Request for Public Comment Regarding Parts 3 and 4 Rules of Practice Rulemaking—P072194, at 4 (Nov. 6, 2008).

89. The Antitrust Section explained that its "primary concern is that by 'codifying' the Commission's right to interject itself into prehearing case management, it may undermine the integrity of the process, compromise the ALJ, and create an appearance of unfairness." Id. at 12. The Antitrust Section also said the FTC's amendments "could reduce the quality of decision making, and may color the perception of the fairness and impartiality of Commission proceedings—a particularly important issue considering that when hearing an appeal, federal courts will give deference to a final FTC decision." Id. at 11.

90. The U.S. Chamber of Commerce added that "it appears that the proposed changes are being rushed into place and for the purpose of giving the FTC material, tactical, and procedural advantage . . . ." U.S. Chamber of Commerce, Comment, Re: Parts 3 and 4 Rules of Practice Rulemaking—P072104, at 1 (Nov. 6, 2008). In fact:

> The FTC's proposed regulations work to effectively eliminate the role of the independent Administrative Law Judge (ALJ) to manage and prepare an initial decision for a case. This results in the elimination of a vital check on potential unfairness inherent in the FTC's administrative procedure. Under the FTC's process, the Commissioners act as both prosecutor and judge in administrative trials. Thus, the same individuals who decide to issue the complaint also decide the final appeal of the administrative trial. With such a clear potential for unfairness or conflict of interest at the forefront of FTC administrative adjudication, it is necessary to preserve some sort of fairness check.

Id. at 2.

91. Under current Commission Rule 3.22(a), "[m]otions to dismiss filed before the evidentiary hearing, motions to strike, and motions for summary decision shall be directly referred to the Commission and shall be ruled on by the Commission unless the Commission in its discretion refers the motion to the Administrative Law Judge."

92. In excess of their authority and in violation of the Constitution's guarantee of due process, the FTC has assumed for itself the power to legislate, to prosecute, and to judge LabMD without even specifying in advance the elements of the data-security offense LabMD has allegedly committed.

93. The empirical evidence demonstrates that the FTC's administrative process is a rigged exercise in futility for LabMD and others similarly situated.

94. According to Commissioner Wright:

> The FTC has voted out a number of complaints in administrative adjudication that have been tried by administrative law judges ("ALJs") in the past nearly twenty years. In each of those cases, after the administrative decision was appealed to the Commission, the Commission ruled in favor of FTC staff. In other words, in 100 percent of cases where the ALJ ruled in favor of the FTC, the Commission affirmed; and in 100 percent of the cases in which the ALJ ruled against the FTC, the Commission reversed.

Joshua D. Wright, Comm'r, Fed. Trade Comm., Recalibrating Section 5: A Response to the CPI Symposium, CPI Antitrust Symposium, at 4 (November 2013), available at

http://www.ftc.gov/sites/default/files/documents/public_statements/recalibrating-section-5-response-cpi-symposium/1311section5.pdf (last visited Mar. 18, 2014).

95. Further administrative proceedings are exhausted and futile.

V. The Irreparable Harm Done By The FTC To LabMD.

96. FTC's power-grab has destroyed LabMD's customer relationships and, in large measure, driven LabMD to cease accepting new specimen samples. But for all of the time, attention, and money LabMD has been forced to devote to addressing the FTC's actions, the company would almost certainly be accepting new specimen samples and providing cancer-diagnostic services to doctors to this day.

97. LabMD, and its doctors, have been denied insurance coverage as a direct result of the FTC's ongoing persecution of the company. For example, One Beacon (a medical malpractice insurance company) recently denied LabMD, and its doctors, coverage, saying: "[W]e are unable to offer ERP terms for the entity [LabMD], and as a result, the individual physicians so I will be closing the file. The potential volatility due to the FTC investigation is something we want to stay away from particularly because it pertains to medical records."

98. LabMD's general liability insurance carrier is planning to non-renew its insurance policy effective May 6, 2014.

99. The FTC's personnel have intentionally interfered with LabMD's customer relationships and effectively engaged in a campaign of commercial disparagement.

100. The FTC's actions have caused, and continue to cause, irreparable injury to LabMD's business reputation and good will in the marketplace.

101. The FTC, Mr. Sheer, and other FTC employees have intentionally set out to destroy LabMD's commercial brand, reputation, and good will.

102. The FTC, Mr. Sheer, and others have caused and continue to cause LabMD irreparable harm far beyond mere litigation expenses and threaten the viability of LabMD's business operations. Much of this harm cannot be quantified in monetary terms, and cannot be remedied by monetary damages. For example, on January 6, 2014, LabMD notified its customers that it would no longer be accepting new specimen samples for testing for the foreseeable future, effective January 11, 2014.

CLAIMS FOR RELIEF

First Claim for Relief
(For Violation of the APA)

103. LabMD repeats paragraphs 4-5, 8-10, 16-19, 21-22, 27-32, 41-50, 54-61, 64-66, 69-81, 84, and 93-95.

104. The FTC's action against LabMD is arbitrary, capricious, an abuse of discretion and power, in excess of statutory authority and short of statutory right, and contrary to law and constitutional right, in violation of 5 U.S.C. § 706.

105. The FTC does not have jurisdiction to regulate LabMD's patient-information data-security and thus its actions are ultra vires.

106. The Commission's orders denying the jurisdictional, ultra vires, and due process claims raised in LabMD's motion to dismiss and LabMD's motion for a stay are both "final agency actions" within the meaning of 5 U.S.C. § 704 and thus LabMD's APA claims are ripe and reviewable now. TVA v. Whitman, 336 F.3d 1236, 1248 (11th Cir. 2004); see, e.g., CSI Aviation Servs. v. DOT, 637 F.3d 408, 411-14 (D.C. Cir. 2011); see Sackett, 132 S. Ct. at 1371-72; see also Athlone Indus., Inc. v. CPSC, 707 F.2d 1485, 1487-88 (D.C. Cir. 1983).

107. LabMD has exhausted all administrative remedies with respect to its jurisdictional and constitutional due-process arguments, which the Commission formally rejected on January 16, 2014.

108. In addition, only administrative remedies providing a genuine opportunity for adequate relief need be exhausted, and here exhaustion is also independently not required because the administrative process is futile and inadequate and LabMD will continue to suffer irreparable harm unless its claims are reviewed by

an Article III Court now. See N.B. by D.G. v. Alachua Cnty. Sch. Bd., 84 F.3d 1376, 1379 (11th Cir. 1996); Porter v. Schweiker, 692 F.2d 740, 742-43 (11th Cir. 1982); Randolph-Sheppard Vendors of Am. v. Weinberger, 795 F.2d 90, 107-08 (D.C. Cir. 1986) (irreparable harm excuses exhaustion).

109. Therefore, the FTC's enforcement action against LabMD should be enjoined and a declaration issued that it lacks authority to regulate patient information data-security.

Second Claim for Relief
(For Ultra Vires Agency Action)

110. LabMD repeats paragraphs 4-5, 8-10, 16-19, 21-22, 27-32, 41-50, 61, 70-81, and 93-96.

111. Regardless of the presence vel non of "final agency action" under 5 U.S.C. § 704, this Court has jurisdiction to adjudicate LabMD's nonstatutory ultra vires and constitutional claims, for the presence or absence of "final agency action" has no jurisdictional effect. See, e.g., Trudeau v. FTC, 456 F.3d 178 (D.C. Cir. 2006); Muniz-Muniz v. U.S. Border Patrol, No. 12-4419, 2013 U.S. App. LEXIS 25400, at *11 (6th Cir. Dec. 20, 2013) (noting that "all of our sister circuits" have concluded 5 U.S.C. § 704 has no effect on a federal-question jurisdiction to adjudicate non-APA claims); see also Arbaugh v. Y & H Corp., 546 U.S. 500, 511, 516-17 (2006).

112. Thus, the FTC's ultra vires actions are ripe for judicial review now regardless of the reviewability of LabMD's APA claims.

113. Exhaustion is not required for these claims under any circumstances. See XYZ Law Firm v. FTC, 525 F. Supp. 1235, 1237 (N.D. Ga. 1981).

114. The FTC's actions against LabMD exceed the power given to it in Section 5 and are thus ultra vires.

115. Judicial review of this claim is available because the Defendant's ultra vires actions exceed the authority conferred on it by Congress and the United States Constitution.

116. Moreover, inter alia, the FTC has effectively violated three specific and mandatory restraints on its Section 5 "unfairness" power.

117. First, the FTC's abuse exceeds its delegated powers and is contrary to specific the FTC Act's prohibitions on the use of consent orders and speeches to create a binding "common law" of data security. 15 U.S.C. § 45(m)(1)(B).

118. Second, in addition to the fact that Congress has not given the FTC Section 5 "unfairness" authority to regulate data security, let alone authority to over-file HHS and regulate PHI data security, the FTC has also independently violated 15 U.S.C. § 45(n)'s specific limits on its Section 5 "unfairness" authority. 15 U.S.C. § 45(n) explicitly states that the Defendant "shall have no authority under this section

or section 18 [15 U.S.C. § 57a] to declare unlawful an act or practice on the grounds that such act or practice is unfair" under the circumstances of this case. 15 U.S.C. § 45(n) further explicitly bars the FTC from using its public policy views as a primary basis for exercising its unfairness authority.

119. Third, the FTC's sworn responses to LabMD's discovery requests demonstrate it is seeking to enforce against LabMD random Internet postings, e-mail alerts, Commission staff reports, and congressional testimony they say establish data-security standards LabMD should have followed, even those these documents do not have the force of law and were not even published in the Federal Register, and they do not allege that LabMD had actual knowledge of any of these Internet postings and other materials. 5 U.S.C. § 552(a)(1).

120. FTC's unauthorized actions are the direct and proximate cause of LabMD's injuries, as described above. Therefore, LabMD is entitled to the declaratory and injunctive relief requested herein.

Third Claim for Relief
(For Fair-Notice Due Process Violations)

121. LabMD repeats paragraphs 4-5, 7-10, 46-49, 74-80, 84-85, and 118-119.

122. This Court has jurisdiction over LabMD's fair-notice due process claim now. Exhaustion is not required for these claims under any circumstances.

123. The Fifth Amendment to the United States Constitution states that "[n]o person shall be . . . deprived of life, liberty, or property, without due process of law." U.S. Const. amend. V.

124. The draft notice order ("Commission Notice Order") if made effective, will be in place for twenty (20) years and, inter alia, require LabMD to (1) "establish and implement, and thereafter maintain, a . . . security program"; (2) "obtain initial and biennial assessment and reports" from third parties for a period of twenty (20) years; (3) provide Commission-approved notice to the individuals listed in the accounts-receivable file and their health insurance companies of Tiversa's actions via first-class mail; (4) deliver copies of the Commission Notice Order to "current and future principals, officers, directors, and mangers," as well as deliver copies to many current and future employees, agents, representatives, and business entities; (5) notify the FTC in writing at least thirty (30) days before making numerous changes, such as change in corporate name or address; and (6) prepare and file detailed reports with the FTC.

125. Additionally, the FTC has reserved the right to order such other relief as it finds necessary and appropriate if it decides that the Commission Notice Order is insufficient, including seeking "restitution" and other types of relief authorized by Section 19 of the Federal Trade Commission Act, 15 U.S.C. § 57b (civil actions for

violations of rules and cease and desist orders respecting unfair or deceptive acts or practices), including but not limited to rescission or reformation of contracts and payment of monetary damages.

126. Under 15 U.S.C. § 45(l), each violation of the FTC cease and desist orders carries up to a $10,000 civil penalty.

127. FTC's actions, January 16 Order, December 13 Order, and the Commission Complaint and Notice Order, thus implicate LabMD's property rights, which are protected by the Due Process Clause of the Fifth Amendment.

128. FTC's refusal to promulgate any regulations or to issue any other guidelines clarifying and providing any notice, let alone constitutionally adequate notice, of what data-security practices they believe Section 5 forbids or requires, or to otherwise establish any meaningful standards, violates LabMD's due process rights.

129. Due process requires that laws that 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); Connally v. Gen. Constr. Co., 269 U.S. 385, 391-95 (1926).

130. This constitutional fair-notice requirement has been thoroughly incorporated into administrative law to limit agencies' ability to regulate past conduct through after-the-fact enforcement actions. Georgia Pac. Corp. v. OSHRC, 25 F.3d 999, 1005 (11th Cir. 1994). Fair-notice due process requirements thus apply to the

FTC administrative enforcement actions seeking to impose cease and desist orders for alleged violations of Section 5.

131. The FTC has failed to meet its burden of establishing reasonably ascertainable standards for what data-security practices it believes Section 5 to either forbid or to require. See Georgia Pac. Corp., 25 F.3d at 1005; Trinity Broad. of Fla., Inc. v. FCC, 211 F.3d 618, 628-32 (D.C. Cir. 2000).

132. Basic principles of due process limit the FTC's "discretion" to enforce Section 5 through administrative adjudications; specifically, the FTC can proceed by adjudication only if it has already provided the baseline level of fair notice that the Constitution requires. The FTC has failed to provide LabMD the baseline level of fair notice of the data-security practices it believes to be required or forbidden by Section 5's "unfairness" language.

133. Because the FTC's Section 5 PHI data-security regulatory scheme forbids or requires the doing of an act in terms so vague that men and women of common intelligence must necessarily guess at its meaning and differ as to its application, it violates due process.

134. In addition, even if the FTC's "reasonableness" standard for PHI data security otherwise passed constitutional muster, the FTC's failure to link its data-security standards to medical-industry standards independently violates due process.

135. FTC's pattern and practice of fair-notice due process violations, as applied to LabMD and all similarly situated, including the defendants in FTC v. Wyndham, violates due process.

Fourth Claim for Relief
(For Facial, Structural Due Process Violations)

136. LabMD repeats paragraphs 4-5, 7-10, 17-19, 23-34, and 84-96.

137. Exhaustion of administrative remedies is not required for facial and structural due process challenges. See, e.g., Matthews v. Eldridge, 424 U.S. 319, 329-32 (1976); Amos Treat & Co. v. SEC, 306 F.2d 260, 267 (D.C. Cir. 1963).

138. The substantial private interests affected by the FTC's actions, the high risk of erroneous deprivation of LabMD's property interests, and the high value of additional procedural safeguards outweigh the FTC's de minimis interest in the existing procedures. Therefore, LabMD has not been provided the procedural safeguards that it is constitutionally entitled to have.

139. Due process minimally requires a fair trial in a fair tribunal and "this applies to administrative agencies which adjudicate as well as to courts." Withrow v. Larkin, 421 U.S. 35, 46-47 (1975).

140. FTC's modifications to its Rules of Practices transgress constitutional limits on blending of prosecutorial, legislative, and adjudicative functions and deprive

all respondents of a fair administrative hearing. Therefore, the Commission's Rules facially and structurally violate due process.

141. Furthermore, the FTC's ex post facto enforcement action against LabMD for alleged violations of unspecified data-security standards in a proceeding in which the FTC acts in a legislative, prosecutorial, and adjudicative capacity further violates due process.

142. Finally, the FTC has predetermined this matter, denying LabMD its right to a fair and level review, including a fair hearing on its Motion to Dismiss before an impartial ALJ.

143. FTC's intentional violations of LabMD's due process rights has caused LabMD hundreds of thousands of dollars in actual damages, harmed its business reputation, caused it to lose good will and business opportunities, and brought the company to the brink of ruin.

Fifth Claim for Relief

(For Retaliation Against LabMD for Protected First Amendment Speech)

144. LabMD repeats paragraphs 4-5, 7-11, 23-49, and 53.

145. The First Amendment to the United States Constitution guarantees LabMD freedom of speech.

146. Mr. Daugherty's book, his webpage about the book, and his speeches and statements about the FTC's actions are political speech and speech about matters of public concern and thus protected by the First Amendment.

147. On information and belief, the FTC's actions against LabMD were retaliation for protected speech by Mr. Daugherty.

148. The FTC's actions against LabMD, as set forth herein, will likely chill a person of ordinary firmness from engaging in the protected First Amendment activity.

149. On information and belief, the FTC's conduct herein was precisely intended and designed, at least in part, to punish LabMD and chill government criticism by LabMD and others targeted by the government.

150. Even if the FTC, Complaint Counsel, and other FTC employees disagree with and find Mr. Daugherty's statements about their actions to be patently offensive, they are not allowed retaliate by bringing an enforcement action against LabMD.

RELIEF REQUESTED

WHEREFORE LabMD requests the following relief:

A. That the Court enter a declaratory judgment that (1) the FTC lacks statutory authority to regulate patient-information data-security practices under Section 5; (2) the FTC's efforts to regulate patient information are ultra vires; (3) the FTC violated LabMD's due process rights by failing to provide constitutionally

adequate notice of what data-security practices the Commission believed Section 5 to forbid or require before the Complaint was filed; (4) the FTC violated LabMD's due process rights by unconstitutionally combining legislative, prosecutorial, investigative, and adjudicatory functions by, among other things, allowing FTC Commissioners to rule on dispositive motions concerning complaints they recently voted to issue; and (5) the FTC unconstitutionally retaliated against LabMD for engaging in constitutionally protected speech.

B. That the Court enter preliminary and permanent injunctive relief providing that the FTC, its agents, servants, employees, and attorneys, and anyone who is in active concert or participation with any of them, shall take no further actions in connection with administrative proceedings known as In the Matter of LabMD, FTC Dkt. No. 9357, including but not limited to issuing orders, holding hearings, taking discovery, and filing motions.

C. That the Court enter preliminary and permanent injunctive relief providing that the FTC, its agents, servants, employees, and attorneys, and anyone who is in active concert or participation with any of them, shall not (1) initiate any civil or administrative enforcement action against LabMD or any other person on the ground that their patient information data-security practices are "unfair" in violation of Section 5; (2) investigate whether LabMD's or any other person's patient

information data-security practices violate Section 5 for "unfairness"; (3) attempt to establish substantive data-security standards under Section 5 and/or enforce Section 5 in civil or administrative proceedings; or (4) undertake or pursue any administrative enforcement proceedings until the Commission amends its Rules of Practice to provide constitutionally adequate due process.

D. That the Court award LabMD its attorneys' fees and litigation costs under the Equal Access to Justice Act and/or such other applicable law.

E. Such other and further relief as this Court deems just and proper.

Respectfully submitted, this 20th day of March, 2014.

/s/ Ronald L. Raider

KILPATRICK TOWNSEND
& STOCKTON LLP
1100 Peachtree Street, NE
Suite 2800
Atlanta, Georgia 30309
Telephone (404) 815-6500
Facsimile (404) 815-6555
rraider@kilpatricktownsend.com
bsingleton@kilpatricktownsend.com
bmeyer@kilpatricktownsend.com

Ronald L. Raider
Georgia Bar No. 592192
Burleigh L. Singleton
Georgia Bar No. 649084
William D. Meyer
Georgia Bar No. 950008

Counsel for Plaintiff

OF COUNSEL:

Reed D. Rubinstein
(applying for admission pro hac vice)
D.C. Bar No. 440153
Dinsmore & Shohl, L.L.P.
801 Pennsylvania Ave., NW, Suite 610
Washington, D.C. 20004
Telephone: 202.372.9120
Fax: 202.372.9141
reed.rubinstein@dinsmore.com

Senior Vice President for Litigation and Counsel to Cause of Action

Michael D. Pepson
(applying for admission pro hac vice)
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.4232
Fax: 202.330.5842
michael.pepson@causeofaction.org
Admitted only in Maryland.
Practice limited to cases in federal court and administrative proceedings before federal agencies.

Dated: March 20, 2014

Verification

I am Michael Daugherty, owner and CEO of LabMD, Inc., which is the plaintiff in this action.

I have read the foregoing Complaint and verify and declare on behalf of LabMD, Inc., under penalty of perjury, that its factual allegations are true, except to those matters stated on information and belief, and as to those matters I believe them to be true to the best of my knowledge.

LabMD, Inc.

By: _____ Date: 3/19/14
Michael Daugherty

LOCAL RULE 7.1 CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing pleading filed with the Clerk of Court has been prepared in 14 point Times New Roman font in accordance with Local Rule 5.1(C).

Dated: March 20, 2014.

/s/ Ronald L. Raider
Ronald L. Raider

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LabMD, INC.,	
Plaintiff,	
v.	Civil Action No. 1:13-cv-01787
FEDERAL TRADE COMMISSION et al.	Hon. Colleen Kollar-Kotelly
Defendants.	

NOTICE OF VOLUNTARY DISMISSAL WITHOUT PREJUDICE

Pursuant to Fed. R. Civ. P. 41(a)(1)(A)(i), Plaintiff LabMD, Inc. (LabMD), by and through its counsel, hereby gives notice of its voluntary dismissal of this case without prejudice.

1. On November 14, 2014, LabMD filed a Verified Complaint for Declaratory and Injunctive Relief, Dkt. No. 1, in this Court.

2. Defendants have not answered or moved for summary judgment.

3. Fed. R. Civ. P. 41(a)(1)(A)(i) provides that so long as the opposing party has not yet served either an answer or motion for summary judgment in response to the complaint, a plaintiff may voluntarily dismiss his case without a court order by filing a notice of dismissal. *Little v. Trott & Trott, P.C.*, 2009 U.S. Dist. LEXIS 116575, *2 (D.D.C. Dec. 14, 2009) (citing Fed. R. Civ. P. 41(a)(1)(A)(i)); *accord Miniter v. Sun Myung Moon*, 736 F. Supp. 2d 41, 44-45 & n. 7. (D.D.C. 2010).

4. Plaintiff hereby gives such notice of voluntary dismissal.

5. Therefore, this action should be dismissed without prejudice. *See, e.g., Little*, 2009 U.S. Dist. LEXIS 116575 at *3 ("As such, Plaintiff's complaint is automatically DISMISSED WITHOUT PREJUDICE without the need for a court order." (citing Fed. R. Civ. P. 41(a)(1)(A)(i) and emphasis in original)).

Respectfully submitted,

/s/ Reed D. Rubinstein
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

Daniel Z. Epstein
D.C. Bar No. 1009132
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Telephone: (202) 499-4232
daniel.epstein@causeofaction.org.

Michael D. Pepson
Cause of Action
1919 Pennsylvania Ave., NW, Suite 650
Washington, D.C. 20006
Phone: 202.499.2024
Fax: 202.330.5842
Email: michael.pepson@causeofaction.org
Admitted only in Maryland. Admitted pro hac vice.
Practice limited to cases in federal court and
administrative proceedings before federal agencies.

Counsel for Plaintiff LabMD

Dated: February 19, 2014

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

FEDERAL TRADE COMMISSION,	)	
	)	
PETITIONER	)	
	)	**CIVIL ACTION FILE NO.:**
v.	)	**1:12-CV-3005-WSD**
	)	
LABMD, INC.,	)	
and MICHAEL J. DAUGHERTY	)	
	)	
RESPONDENTS	)	

RESPONSE TO PETTIONER'S PETITION TO ENFORCE CIVIL INVESTIGATIVE DEMANDS

COMES NOW LABMD, INC. ("LabMD") and Michael J. Daugherty ("Daugherty")(collectively "Respondents") and hereby file this Response to Petition for the Federal Trade Commission to show this Honorable Court the Following:

1.

Respondents hereby agree that the Federal Trade Commission ("FTC") is an administrative agency of the United States. As the remaining allegations referenced in Paragraph 1 are statements of law, all remaining allegations contained in Paragraph 1 are hereby denied.

2.

All allegations contained in Paragraph 2 are hereby denied as the statutes speak for themselves.

3.

Respondents deny the allegations contained in Paragraph 3. The FTC has no jurisdiction over Respondents based upon its inquiry. By way of further response, LabMD denies the allegations contained in Paragraph 3 as the statute speaks for itself.

4.

Respondents admit the allegations contained in the first sentence of Paragraph 4. Respondents deny the allegations as stated in the second sentence. LabMD only performs medical testing in the State of Georgia. Furthermore, LabMD does not treat patients. It is a medical testing facility that tests tissue samples, urine and blood from patients across the United States. Respondents admit Michael J. Daugherty is the owner and president of LabMD. Respondents deny they are engaged in commerce throughout the country. Respondents deny all remaining allegations contained in Paragraph 4 as the statutes speak for themselves.

5.

Respondents admit that on January 3, 2008, the FTC issued a resolution File No P954807 ("Petition"). Respondents deny the remaining allegations as the Petition speaks for itself.

6.

Respondents deny the allegations contained in Paragraph 6. By way of further response, Respondents note that the FTC, in concert with Tiversa and Dartmouth College, began remotely logging into private citizens computer networks trolling for medical files containing personally identifiable information and sensitive health information and none of Respondents' information was available on "easily-accessible peer-to-peer ("P2P") file sharing networks." Furthermore, Respondents are without sufficient information to either admit or deny the allegations contained in Paragraph 6 and, as such, deny the allegations. Finally, the statute speaks for itself and, as such, the allegations contained in Paragraph 6 are hereby denied.

7.

Respondents are without sufficient information to either admit or deny the allegations contained in Paragraph 7 and, as such, deny the allegations contained in Paragraph 7. By way of further response, the FTC has utterly failed to articulate what "reasonable data security measures" or what the "other statutes or regulations enforced by the Commission" are. Finally, the FTC staff's "consultation with several third parties with expertise in P2P networks" included Tiversa, a private, for-profit corporation which secured funding from the federal government under the Department of Homeland Security.

8.

Respondents are without sufficient information to either admit or deny the allegations contained in Paragraph 8 and, as such, the allegations are hereby denied. By way of further response, Respondents note that Tiversa, the party funded by the federal government, provided the FTC with the 1,718 File. Respondents deny that the 1,718 File contained medical treatment codes.

9.

Respondents are without sufficient information to either admit or deny the allegations contained in Paragraph 9 and, as such, the allegations are hereby denied. Respondents further deny that the FTC issued a "voluntary access requests" to LabMD.

10.

Respondents deny the allegations contained in sentence 1 of Paragraph 10 and by way of further response allege that Respondents provided no less than six written responses to the FTC including correspondence, paper files, CD data files with over 5,000 pages of data, two in-person meetings with the FTC and numerous telephone conversations with the FTC staff. Respondents admit that the FTC issued two separate CIDs to LabMD but deny all remaining allegations contained in Paragraph 10.

11.

Respondents deny the allegations contained in Paragraph 11 as the CIDs speak for themselves.

12.

Respondents deny the allegations contained in Paragraph 12 as the law speaks for itself.

13.

Respondents admit the allegations contained in Paragraph 13.

14.

Respondents admit that the FTC denied the petitions to limit or quash on April 20, 2012 ("April 20 Ruling"). The April 20, 2012 Ruling speaks for itself and, as such, all remaining allegations are denied.

15.

Respondents admit that they submitted a request for review by the full FTC and that on June 21, 2012, the FTC affirmed the April 20 Ruling. Respondents deny all remaining allegations contained in Paragraph 15 as the respective documents speak for themselves.

16.

Respondents admit the FTC staff contacted respondents on June 25, 2012 and that Respondents submitted a letter to the FTC staff on June 29, 2012. Respondents deny all remaining allegations contained in Paragraph 16.

17.

Respondents deny the allegations contained in Paragraph 17.

WHEREFORE, Respondents respectfully request that this Honorable Court:

1. deny the FTC's request for an order requiring Respondents to comply with the CIDs; and
2. for such other relief as this Court deems just and proper.

Respectfully submitted this 14th Day of September, 2012

/s/ Stephen F. Fusco

Stephen F. Fusco
Georgia Bar No. 281030
2030 Powers Ferry Road; Suite 520
Atlanta, Georgia 30339
sfusco@labmd.org
(678) 443-2343 – phone
(404) 601-9977

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

FEDERAL TRADE COMMISSION,	)	
	)	
PETITIONER	)	
	)	**CIVIL ACTION FILE NO.:**
v.	)	**1:12-CV-3005-WSD**
	)	
LABMD, INC.,	)	
and MICHAEL J. DAUGHERTY	)	
	)	
RESPONDENTS	)	

CERTIFICATE OF SERVICE, FONT, AND MARGINS

I hereby certify that on September 14, 2012, I electronically filed the foregoing *Response to Petition of the Federal Trade Commission For an Order to Enforce Civil Investigative Demands* with the Clerk of the Court using the CM/ECF System, which sent notification of such filing to all counsel of record.

I further certify that I prepared this document in 13 point Book Antiqua font and complied with the margin and type requirements of this Court.

/s/ Stephen F. Fusco
Stephen F. Fusco

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

FEDERAL TRADE COMMISSION,	)	
	)	
PETITIONER	)	
	)	**CIVIL ACTION FILE NO.:**
v.	)	**1:12-CV-3005-WSD**
	)	
LABMD, INC.,	)	
and MICHAEL J. DAUGHERTY	)	
	)	
RESPONDENTS	)	

RESPONSE TO PETTIONER'S PETITION TO ENFORCE CIVIL INVESTIGATIVE DEMANDS

COMES NOW LABMD, INC. ("LabMD") and Michael J. Daugherty ("Daugherty")(collectively "Respondents") and hereby file this Response to Petition for the Federal Trade Commission to show this Honorable Court the Following:

1.

Respondents hereby agree that the Federal Trade Commission ("FTC") is an administrative agency of the United States. As the remaining allegations referenced in Paragraph 1 are statements of law, all remaining allegations contained in Paragraph 1 are hereby denied.

2.

All allegations contained in Paragraph 2 are hereby denied as the statutes speak for themselves.

3.

Respondents deny the allegations contained in Paragraph 3. The FTC has no jurisdiction over Respondents based upon its inquiry. By way of further response, LabMD denies the allegations contained in Paragraph 3 as the statute speaks for itself.

4.

Respondents admit the allegations contained in the first sentence of Paragraph 4. Respondents deny the allegations as stated in the second sentence. LabMD only performs medical testing in the State of Georgia. Furthermore, LabMD does not treat patients. It is a medical testing facility that tests tissue samples, urine and blood from patients across the United States. Respondents admit Michael J. Daugherty is the owner and president of LabMD. Respondents deny they are engaged in commerce throughout the country. Respondents deny all remaining allegations contained in Paragraph 4 as the statutes speak for themselves.

5.

Respondents admit that on January 3, 2008, the FTC issued a resolution File No P954807 ("Petition"). Respondents deny the remaining allegations as the Petition speaks for itself.

6.

Respondents deny the allegations contained in Paragraph 6. By way of further response, Respondents note that the FTC, in concert with Tiversa and Dartmouth College, began remotely logging into private citizens computer networks trolling for medical files containing personally identifiable information and sensitive health information and none of Respondents' information was available on "easily-accessible peer-to-peer ("P2P") file sharing networks." Furthermore, Respondents are without sufficient information to either admit or deny the allegations contained in Paragraph 6 and, as such, deny the allegations. Finally, the statute speaks for itself and, as such, the allegations contained in Paragraph 6 are hereby denied.

7.

Respondents are without sufficient information to either admit or deny the allegations contained in Paragraph 7 and, as such, deny the allegations contained in Paragraph 7. By way of further response, the FTC has utterly failed to articulate what "reasonable data security measures" or what the "other statutes or regulations enforced by the Commission" are. Finally, the FTC staff's "consultation with several third parties with expertise in P2P networks" included Tiversa, a private, for-profit corporation which secured funding from the federal government under the Department of Homeland Security.

8.

Respondents are without sufficient information to either admit or deny the allegations contained in Paragraph 8 and, as such, the allegations are hereby denied. By way of further response, Respondents note that Tiversa, the party funded by the federal government, provided the FTC with the 1,718 File. Respondents deny that the 1,718 File contained medical treatment codes.

9.

Respondents are without sufficient information to either admit or deny the allegations contained in Paragraph 9 and, as such, the allegations are hereby denied. Respondents further deny that the FTC issued a "voluntary access requests" to LabMD.

10.

Respondents deny the allegations contained in sentence 1 of Paragraph 10 and by way of further response allege that Respondents provided no less than six written responses to the FTC including correspondence, paper files, CD data files with over 5,000 pages of data, two in-person meetings with the FTC and numerous telephone conversations with the FTC staff. Respondents admit that the FTC issued two separate CIDs to LabMD but deny all remaining allegations contained in Paragraph 10.

11.

Respondents deny the allegations contained in Paragraph 11 as the CIDs speak for themselves.

12.

Respondents deny the allegations contained in Paragraph 12 as the law speaks for itself.

13.

Respondents admit the allegations contained in Paragraph 13.

14.

Respondents admit that the FTC denied the petitions to limit or quash on April 20, 2012 ("April 20 Ruling"). The April 20, 2012 Ruling speaks for itself and, as such, all remaining allegations are denied.

15.

Respondents admit that they submitted a request for review by the full FTC and that on June 21, 2012, the FTC affirmed the April 20 Ruling. Respondents deny all remaining allegations contained in Paragraph 15 as the respective documents speak for themselves.

16.

Respondents admit the FTC staff contacted respondents on June 25, 2012 and that Respondents submitted a letter to the FTC staff on June 29, 2012. Respondents deny all remaining allegations contained in Paragraph 16.

17.

Respondents deny the allegations contained in Paragraph 17.

WHEREFORE, Respondents respectfully request that this Honorable Court:

1. deny the FTC's request for an order requiring Respondents to comply with the CIDs; and
2. for such other relief as this Court deems just and proper.

Respectfully submitted this 14th Day of September, 2012

/s/ Stephen F. Fusco

Stephen F. Fusco
Georgia Bar No. 281030
2030 Powers Ferry Road; Suite 520
Atlanta, Georgia 30339
sfusco@labmd.org
(678) 443-2343 – phone
(404) 601-9977

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

FEDERAL TRADE COMMISSION,	)	
	)	
PETITIONER	)	
	)	**CIVIL ACTION FILE NO.:**
v.	)	**1:12-CV-3005-WSD**
	)	
LABMD, INC.,	)	
and MICHAEL J. DAUGHERTY	)	
	)	
RESPONDENTS	)	

CERTIFICATE OF SERVICE, FONT, AND MARGINS

I hereby certify that on September 14, 2012, I electronically filed the foregoing *Response to Petition of the Federal Trade Commission For an Order to Enforce Civil Investigative Demands* with the Clerk of the Court using the CM/ECF System, which sent notification of such filing to all counsel of record.

I further certify that I prepared this document in 13 point Book Antiqua font and complied with the margin and type requirements of this Court.

/s/ Stephen F. Fusco
Stephen F. Fusco

In the Matter of LabMD, Inc.
Docket No. 9357
Statement of Commissioner Julie Brill
December 24, 2013

On August 28, 2013, the Commission voted unanimously to issue an administrative complaint against LabMD, Inc. ("LabMD"). The complaint alleges that LabMD exposed consumers' sensitive personal information to unauthorized disclosure through its failure to provide reasonable and appropriate security for that information. As a result, the complaint alleges, LabMD engaged in an "unfair act or practice," in violation of FTC Act § 5(a), 15 U.S.C. § 45(a). *See Complaint, at* 2-5 (¶¶ 6-23). LabMD denies that it violated the FTC Act. *See LabMD's Answer and Defenses to Administrative Complaint, at* 5 (¶¶ 22-23) (Sept. 17, 2013).

On November 12 and November 26, 2013, LabMD filed two separate motions to stay the Commission's administrative proceeding while LabMD seeks review in two federal courts of the propriety of the Commission's administrative action against LabMD. *See generally Motion to Dismiss Complaint with Prejudice and to Stay Administrative Proceedings* (Nov. 12, 2013); *Motion to Stay Proceedings Pending Review in the U.S. Court of Appeals for the Eleventh Circuit and the U.S. District Court for the District of Columbia* (Nov. 26, 2013). LabMD brought the first of these federal court actions through a Verified Complaint for Declaratory Relief against the Commission filed in the U.S. District Court for the District of Columbia on November 14, 2013. On November 18, 2013, LabMD filed a "Petition for Review of Unlawful Federal Trade Commission Attempt to Regulate Patient-Information" in the U.S. Court of Appeals for the Eleventh Circuit. On December 13, 2013, the Commission unanimously denied LabMD's motions to stay the Commission's administrative proceeding. *See Order Denying Respondent LabMD's Motions for Stay, at* 1 (Dec. 13, 2013).

On December 17, 2013, four days after the Commission denied LabMD's motions to stay the administrative proceeding, LabMD filed a motion to disqualify me from further participation in this matter ("Motion to Disqualify") on the basis of two speeches I recently delivered about data security and privacy protection in the United States, and the relationship between the U.S. and the European Union with regard to commercial privacy. On December 24, 2013, Complaint Counsel filed an opposition to the Motion to Disqualify. My statement today addresses the Motion to Disqualify. *See* 16 C.F.R. § 4.17(b)(3)(ii).

LabMD's Motion to Disqualify is without merit. In my speeches, I provided an overview of the Commission's enforcement work in the areas of privacy and data security. The Motion to Disqualify focuses on one or two sentences in each of these two speeches. These sentences refer in the most general of terms to the Commission's wide range of enforcement activities. In this context, both speeches note that the Commission has "sued companies" on the basis of their data security practices. The main text does not name a specific company, nor does it discuss the specific facts in any complaint that the Commission has filed.

The only specific reference to LabMD in the two speeches is in the footnotes, which were provided to point readers to supporting documents and resources. Specifically, each speech contains a single footnote that cites the administrative complaint against LabMD as an example

of the Commission's enforcement activity in the data security area. Similarly, the neighboring citations provide examples of other enforcement actions in areas ranging from spam to children's privacy. The clear purpose of the single citation to the administrative complaint against LabMD – as well as the other citations – is to refer readers to enforcement actions that the Commission has brought in its efforts to protect consumers from a variety of privacy and data security harms.

A disinterested reader could not reasonably conclude from these two speeches that I had prejudged either the facts or the legal issues in the LabMD proceeding. *See Metropolitan Council of NAACP Branches v. FCC*, 46 F.3d 1154, 1165 (D.C. Cir. 1995). The speeches cited in the Motion to Disqualify contain no explicit or implicit discussion of any facts at issue in this case, and thus bear no resemblance to the 1968 speech (of the FTC's then-Chairman Dixon) underlying the main judicial precedent on which LabMD relies. *See Cinderella Career & Finishing Schools v. FTC*, 425 F.2d 583, 589-90 (D.C. Cir. 1970). Nor do my speeches contain any discussion of how the legal standard that the Commission applies in data security cases might apply to LabMD. Simply put, the speeches contain no evidence that I had made up my mind about specific factual or legal issues in this case. *See Metropolitan Council*, 46 F.3d at 1164-65 (denying challenge to commissioners' decisions not to recuse themselves).

My speeches are designed to inform the public of the many enforcement activities that the Commission undertakes to protect consumers' privacy and security interests. *See American Medical Ass'n v. FTC*, 638 F.2d 443, 448-49 (2d Cir. 1980). In every matter that comes before the Commission, I review all of the relevant facts and arguments on all sides of the issues before reaching any conclusions. My participation in LabMD is no different. LabMD's references to the footnote citations amount to nothing more than a "vague and flimsy" suggestion to the contrary. *Metropolitan Council*, 46 F.3d at 1165.

Nevertheless, I am concerned that full adjudication of the Motion to Disqualify under Rule 4.17 would likely create an undue distraction from the important issues raised in the Commission's administrative complaint against LabMD. Allowing such a distraction to further complicate or delay adjudication of this matter would not serve the public interest. Accordingly, I recuse myself from further participation in this matter.

ORIGINAL
FEDERAL TRADE COMMISSION
RECEIVED DOCUMENTS
567511
NOV 22 2013
SECRETARY

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

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

ORDER ON RESPONDENT'S MOTION FOR A PROTECTIVE ORDER

I.

On November 5, 2013, Respondent LabMD, Inc. ("Respondent") filed a Motion for a Protective Order ("Motion") pursuant to Commission Rule of Practice 3.31(d), 16 C.F.R. § 3.31(d), seeking an order limiting or barring deposition and document subpoenas issued by Complaint Counsel to various nonparties.[1] Complaint Counsel filed an opposition to the Motion on November 15, 2013 ("Opposition"). For the reasons set forth below, Respondent's Motion is GRANTED in part and DENIED in part.

Respondent's Motion included a request for oral argument on its Motion. That request is DENIED.

II.

A.

The Complaint charges that Respondent, a lab that provides doctors with cancer detection services, engaged in an unfair trade practice in violation of Section 5(a) of the FTC Act. Complaint ¶ 23. Specifically, the Complaint alleges that Respondent failed to maintain adequate network security to protect confidential patient information and that such failure caused, or is likely to cause, substantial consumer injury. Complaint ¶ 22. According to the Complaint, a third party informed Respondent that its June 2007 insurance aging report was available on a peer-to-peer, or "P2P," network through Limewire, a P2P file sharing application. Complaint ¶ 17. This file, the Complaint alleges, contained the names, dates of birth, Social Security

[1] According to the Motion, Respondent seeks protection from subpoenas for deposition and/or documents issued to: Allen Truett, 21st Century Oncology, Alison Simmons, Automated PC Technologies, David Lapides, Cyprus Communications, Eric Knox, Erick Garcia, Jeff Martin, Forensic Strategy Services, Karalyn Garrett, Josie Maldanado, John Boyle, Karina Jestes, Lawrence Hudson, Jeremy Dooley, Managed Data Solutions, Matt Bureau, MasterCard Worldwide, Patrick Howard, ProviDyn, Robert Hyer, Rosalind Woodson, Sacramento Police Dept., Sandy Springs GA Police Depart., Scott Moulton, Trend Micro, Inc., US Bank Nat'l Ass'n, Chris Maire, Visa Inc., Michael Daugherty, and Southeast Urology Network (hereafter, the "Nonparties"). *See* Motion at 2 n.1.

numbers, health insurance policy information, and other alleged confidential information for approximately 9,300 consumers. Complaint ¶ 19. The Complaint further avers:

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

Complaint ¶ 21.

Respondent's Answer admits that the alleged third party, Tiversa Holding Corporation ("Tiversa"), contacted Respondent in May 2008 and claimed to have obtained the P2P insurance aging file via Limewire but denies that Respondent violated the FTC Act or that any consumer was injured by the alleged security breach. Answer ¶¶ 17-23.

B.

The permissible scope of discovery is governed by Commission Rule of Practice 3.31(c), which provides in pertinent part: "Parties may obtain discovery to the extent that it may be reasonably expected to yield information relevant to the allegations of the complaint, to the proposed relief, or to the defenses of any respondent." 16 C.F.R. § 3.31(c)(1). Even if discovery is reasonably expected to yield relevant information, however, discovery "shall be limited by Administrative Law Judge" if he determines that "(i) The discovery sought from a party or third party is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) The party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) The burden and expense of the proposed discovery on a party or third party outweigh its likely benefit." 16 C.F.R. § 3.31(c)(2). In addition, under Rule 3.31(d) the Administrative Law Judge "may also deny discovery or make any other order which justice requires to protect a party or other person from annoyance, embarrassment, oppression, or undue burden or expense, or to prevent undue delay in the proceeding." 16 C.F.R. § 3.31(d).

As more fully discussed below, Respondent objects to certain categories of discovery, on varying grounds, such as relevance and undue burden. Complaint Counsel responds that the subpoenas properly seek information relevant to the allegations of the Complaint, to the proposed relief, and to Respondent's anticipated defenses, and that Respondent has not met its burden of showing that Complaint Counsel should be prevented from conducting relevant nonparty discovery. The burden of demonstrating that the challenged discovery should not proceed is on Respondent, as the proponent of the requested protective order. *In re Polypore Int'l*, 2008 FTC LEXIS 155, at *14-16 (Nov. 14, 2008); *In re Schering-Plough Corp.*, 2001 FTC LEXIS 105, at *5 (July 6, 2001).

As a preliminary matter, however, Complaint Counsel argues that Respondent lacks standing to challenge the subpoenas served on nonparties. Accordingly, Respondent's standing to challenge the discovery is addressed first.

III.

A.

Commission Rule 3.31(d) governing protective orders expressly authorizes protecting "a party or other person" against improper discovery. 16 C.F.R. § 3.31(d). Moreover, in *In re Horizon Corp.*, 88 F.T.C. 208, 1976 FTC LEXIS 209, at *4 n.5 (July 28, 1976), the Commission rejected the argument of complaint counsel in that case that the respondent had no standing to challenge nonparty discovery, stating:

> While a party may not ask for an order to protect the rights of another party or a witness if that party or witness does not claim protection for himself, *see Commercial Laundry v. Linen Supply Assn.*, 90 F. Supp. 470 (S.D.N.Y. 1950); 8 C. Wright & A. Miller, *Federal Practice and Procedure* § 2035 at 261 (1970), he may seek an order if he believes his own interest is jeopardized. *Id.* Respondent, as the subject of an adjudicative proceeding, was entitled to raise its claim that the investigational subpoenas would jeopardize its procedural rights.

In addition, consistent with *Horizon*, numerous federal court jurisdictions permit a party to seek a protective order against discovery issued to nonparties, where the party claims that the discovery interferes with a right or privilege of the party itself, as opposed to the rights or burdens belonging to the subpoenaed nonparties. *Fleet Bus. Credit Corp. v. Hill City Oil Co.*, No. 01-2417, 2002 WL 1483879, at *2 (W.D. Tenn. June 26, 2002) ("Many district courts have acknowledged [Rule 26(c)] allows a party to file a motion for protective order on behalf of a non-party."); *U.S. v. Operation Rescue*, 112 F. Supp. 2d 696, 705 (S.D. Ohio 1999) ("As Plaintiff properly notes, several other federal courts have found that a party has standing to seek a protective order on behalf of non-parties."). *See also* Charles Alan Wright & Arthur R. Miller, Federal Practice and Procedure Civil 2d § 2035 ("A party may not ask for an order to protect the rights of another party or a witness if that party or witness does not claim protection for himself, but a party may seek an order if it believes its own interest is jeopardized by discovery sought from a third person.").

In holding that a party has standing to seek a protective order barring discovery issued to nonparties, courts have relied on the language of Federal Rule of Civil Procedure 26(c) which, similar to Commission Rule 3.31(d), explicitly refers to the right of "a party" as well as "any person from whom discovery is sought" to seek such protection.[2] *Underwood v. Riverview of*

[2] *See* Fed. R. Civ. Pro. 26(c) ("A party or any person from whom discovery is sought may move for a protective order . . . . The court may, for good cause, issue an order *to protect a party or person* from annoyance, embarrassment, oppression, or undue burden or expense, . . .") (emphasis added); Commission Rule 3.31(d) (Administrative Law Judge may "deny discovery or make any other order which justice requires *to protect a party or other person* from annoyance, embarrassment, oppression, or undue burden or expense, or to prevent undue delay in the proceeding.") (emphasis added).

Ann Arbor, 2008 U.S. Dist. LEXIS 107323, at *4 (E.D. Mich. Dec. 15, 2008). *Accord Shukh v. Seagate Tech., LLC*, 2013 U.S. Dist. LEXIS 140159, at *20 (D. Minn. Sept. 30, 2013); *GATX Corp. v. Appalachian Fuels, LLC*, 2011 U.S. Dist. LEXIS 103536, at *15 (E.D. Ky. Sept. 9, 2011).

Moreover, as further explained in *Shukh*, the scope of discovery is limited and a court is obliged to enforce such limitations to protect the rights of a party, even where the discovery is directed at nonparties:

> [Discovery] is limited to "any nonprivileged matter that is relevant to any party's claim or defense." Fed. R. Civ. P. 26(b)(1). The Rule also provides that the court "on motion or on its own . . . must limit the frequency or extent of discovery otherwise allowed" by the Rules if "the discovery sought is unreasonably cumulative or duplicative" or "the burden or expense of the proposed discovery outweighs its likely benefit." Fed. R. Civ. P. 26(b)(2)(C). Where a party, such as Seagate, contends that subpoena requests are irrelevant, cumulative, and burdensome, they are not simply asserting the rights of the third party, but their own right to reasonable discovery and efficient disposition of the case. . . . Because the Court finds that Seagate is entitled, as a party to the litigation, to limit irrelevant and cumulative discovery, the Court concludes that the Magistrate Judge did not err in finding that Seagate had standing to bring its motion for a protective order.

Id. at *22-23. *See also Tarigo v. Aetna Life Ins. Co.*, 2012 U.S. Dist. LEXIS 183800, at *4 (S.D. Fla. Dec. 12, 2012) (holding that party had standing to seek a protective order under Federal Rule of Civil Procedure 26(c) against asserted irrelevant discovery subpoena to nonparty); *White Mule Co. v. ATC Leasing Co. LLC*, 2008 U.S. Dist. LEXIS 51344, at *13-14 (N.D. Ohio June 25, 2008); *Underwood*, 2008 U.S. Dist. LEXIS 107323, at *4-5 (holding that the "purposes of Rule 26(c) encompass the overall limit of Federal Rule of Civil Procedure 26 -- information that is relevant to a claim or defense"); *Auto-Owners Ins. Co. v. Southeast Floating Docks, Inc.*, 231 F.R.D. 426, 429-30 (M.D. Fla. 2005) (deeming defendants' motion to quash as a motion for a protective order under Rule 26(c), and holding that as parties, defendants "clearly have standing to move for a protective order if the [nonparty] subpoenas seek irrelevant information"); *United States v. Operation Rescue*, 112 F. Supp. 2d 696, 705 (S.D. Ohio 1999).[3]

B.

Complaint Counsel acknowledges the governing rule that a party has standing to object to nonparty discovery, provided the party is raising a personal right or privilege of its own, as opposed to the rights of the nonparties, but summarily asserts that Respondent has raised no such rights. Opposition at 4. Therefore, Complaint Counsel contends, Respondent lacks standing to

[3] Where the Federal Rules of Civil Procedure are similar to the Commission's Rules of Practice, those rules and case law interpreting them may be useful, though not controlling, in adjudicating a dispute. *In re POM Wonderful LLC*, 2011 FTC LEXIS 42, at *9 n.3 (Mar. 16, 2011); *In re L.G. Balfour Co.*, 61 F.T.C. 1491, 1492, 1962 FTC LEXIS 367, at *4 (Oct. 5, 1962).

object to the nonparty subpoenas.[4] Having fully reviewed the Motion, Respondent's Motion, at least in part, raises Respondent's own rights with respect to the nonparty discovery, such as irrelevance and undue burden on Respondent. Accordingly, Respondent's motion for protective order will be considered to the extent it is based upon such arguments.

However, Respondent's Motion also includes arguments regarding the rights of, or burdens allegedly placed upon, the nonparties in connection with the requested discovery. For example, Respondent argues that the document subpoenas seek "thousands of documents" from the nonparties "many of which have already been provided by LabMD," and therefore the nonparties should not have to produce such "duplicative" information. Motion at 7-9. Similarly, Respondent notes that it spent "hundreds of hours" complying with document requests similar to those contained in the document subpoenas, and argues that the nonparties should not be required to expend such time and resources, and that in order to avoid this burden, the documents are better obtained from LabMD than from the nonparties. Motion at 8-9. In addition, Respondent asserts that the nonparty depositions should be barred, in part because they are allegedly "duplicative" of the document subpoenas to these nonparties, as well as duplicative of information that Respondent asserts Complaint Counsel already has. Each of the foregoing arguments clearly relies on alleged rights of, and burdens upon, the nonparties, rather than rights of, or burdens upon, Respondent itself. Because the legal authorities discussed above are clear that a party has no standing to obtain a protective order against nonparty discovery on the basis of asserted burdens on the nonparties, particularly where, as here, none of the nonparties has moved to quash the subpoenas, *In re Horizon Corp.*, 1976 FTC LEXIS 209, at *4 n.5, Respondent's arguments in this regard cannot, and will not, be considered.

IV.

A.

The categories of discovery at issue in Respondent's Motion can be generally summarized as follows:

(1) Discovery into the facts and circumstances of a Sacramento, California criminal case in which certain individuals were found in possession of LabMD patient information, and subsequently pled "no contest" to the unauthorized use of personal identifying information (the "Sacramento Incident");

(2) Discovery into any information involving a time period other than 2005-2008;

(3) Discovery into the nature of Respondent's computer network security, including its services contracts and communications with various Information Technology ("IT")

[4] Complaint Counsel cites some cases that appear to set forth an absolute rule that a party can *never* challenge subpoenas issued to nonparties. *See, e.g., US Bank Nat'l Ass'n v. PHL Variable Ins. Co.*, 2012 U.S. Dist. LEXIS 158448 (S.D.N.Y. Nov. 5, 2012); *In re Basic Research LLC*, No. 9318, 2004 FTC LEXIS 237 (Dec. 9, 2004) (ALJ). To the extent that *US Bank* adopts such an absolute rule, it is contrary to numerous other federal jurisdictions and unpersuasive. The Administrative Law Judge's holding in *Basic Research*, because it appears to stand for an absolute prohibition against a party challenging a nonparty subpoena, is contrary to the Commission's holding in *Horizon* and is therefore inapplicable.

service providers;

(4) Discovery into the existence of any security incidents involving Respondent's computer network; and

(5) Discovery regarding a book written by Respondent's CEO Michael Daugherty.[5]

Parties may obtain discovery to the extent that it may be reasonably expected to yield information relevant to the allegations of the complaint, the proposed relief, or the defenses of the respondent. 16 C.F.R. § 3.31(c)(1). Parties resisting discovery of relevant information carry a heavy burden of showing why discovery should be denied. *In re Polypore Int'l*, 2008 FTC LEXIS 155, at *16.

With respect to the Sacramento Incident, Respondent asserts that the individuals found in possession of personally identifiable patient information possessed LabMD's "Day Sheets" and that the "Day Sheets" were available only in hard copy, not on LabMD's computer network. Respondent thus asserts that discovery regarding the Sacramento Incident is not "strongly relevant" to LabMD's computer network security and urges that all subpoenas with respect thereto should, therefore, be barred. Motion at 6-7.[6] Complaint Counsel counters that it anticipates that subpoenas served on individuals with information related to the Sacramento Incident will yield information relevant to consumer injury, which is an element of the law violation alleged in the Complaint. Opposition at 8. Complaint Counsel further contends that because Respondent has asserted that no consumer has suffered injury, these subpoenas are reasonably anticipated to yield information relevant to Respondent's defenses.

Discovery into the Sacramento Incident, as alleged in the Complaint, is reasonably expected to yield information relevant to whether Respondent failed to provide reasonable and appropriate security for personal information on its computer networks and whether consumers suffered injury. Thus, Respondent has not met its burden of showing that discovery on the Sacramento Incident should be denied.

---

[5] Respondent claims that the subpoenas seek a number of categories of discovery that do not, in fact, appear in the topics or specifications attached to the challenged subpoenas. For example, Respondent contends that the subpoenas seek "the names of all Consumers who requested credit monitoring services after receiving a Communication from LabMD related to any Security Incident;" and the "percentage of the total number of Consumers whose samples LabMD has tested . . . who: a. are uninsured, b. have commercial health insurance, c. have Medicare, and d. have Medicaid." Such requests do not appear in the subpoenas. *Compare generally e.g.*, Motion at 8, category nos. 5-6; Motion at 9-10, category nos. 6-7 *with* Motion Exhibit 1. For this reason, Respondent's assertions as to the propriety of such discovery will not be addressed.

[6] Respondent urges that third party subpoenas must have a stronger showing of relevance than party discovery. Motion at 5 & n.9, citing *Echostar Communications Corp. v. News Corp.*, 180 F.R.D. 391, 394 (D. Colo. 1998); *Bio-Vita, Ltd. v. Biopure Corp.*, 138 F.R.D. 13, 17 (D. Mass. 1991). In both *Echostar* and *Bio-Vita*, it was the nonparties who sought the courts' protection from onerous discovery. Critical to each court's decision to impose a higher standard than mere relevance was the weighing of the burden on the nonparties to comply. Here, as discussed above, no nonparty has filed a motion to quash and Respondent does not have standing to protect the rights of the nonparties with respect to the burdens on those nonparties. Thus, case law holding that in order to protect nonparties from intrusive requests, discovery from nonparties must be "strongly relevant" is not applicable.

With respect to discovery into any information involving a time period other than 2005 to 2008, Respondent asserts that LabMD's technology and software, other than that in place at the time of the events in Complaint paragraphs 17-20, is irrelevant. Motion at 7. In its Opposition, Complaint Counsel asserts that LabMD's failures began before 2005 and continued past 2008 and that the subpoenas specify reasonable time periods that are appropriate to the discovery sought. Opposition at 1, 7 n.8.

A request for documents relating to the time period being investigated by Complaint Counsel is relevant. *See In re North Texas Specialty Physicians*, 2004 FTC LEXIS 14, at *4 (Jan. 30, 2004). The Complaint does not allege that Respondent's "failures" began before 2005 and thus discovery of such information does not appear relevant to the allegations of the Complaint. Moreover, with one exception, the instructions on the subpoenas *duces tecum* limit the period covered by a document request to the period from January 1, 2005 or a later period to present.[7]

Information from the time period after 2008 may provide information on whether, in the time period since the alleged security breach, Respondent has employed reasonable and appropriate measures to prevent unauthorized access to personal information and thus may be relevant to the scope of the requested injunctive relief in this case. Accordingly, the subpoenas shall be limited to the period from January 1, 2005 to present.

Regarding discovery into the nature of Respondent's computer network security, including its services contracts and communications with various IT service providers, such information is relevant to whether Respondent failed to provide reasonable and appropriate security for personal information on its computer networks and thus is relevant to the allegations of the Complaint.

With respect to discovery into the existence of any security incidents involving Respondent's computer network, the Complaint alleges as "security incidents" the exposure of the P2P insurance aging file and the Sacramento Incident. It is not apparent that any other security incidents are relevant to the allegations of the Complaint; however, Respondent denies that its security practices caused any consumer injury. Therefore, the existence of other security incidents may be relevant to Respondent's defenses. In addition, the existence of additional security incidents may be relevant to the nature and extent of any appropriate relief in this case, should the alleged violations of the FTC Act be proven. Accordingly, Respondent has failed to demonstrate that the requested discovery is not reasonably likely to lead to the discovery of relevant evidence, or that the requested discovery should otherwise not be allowed.

As to discovery regarding a book written by Respondent's CEO Michael Daugherty, Complaint Counsel states that Mr. Daugherty's book concerns the circumstances relating to the exposure of the P2P insurance aging file and LabMD's business practices. Respondent argues that Mr. Daugherty's self-published manuscript, titled "The Devil Inside the Beltway," is critical of the FTC's conduct with regard to the investigation and litigation of the instant matter, and that the document subpoena to Mr. Daugherty – and Complaint Counsel's nonparty discovery

[7] The only subpoena *duces tecum* seeking documents from the period before 2005 was the one served on Automated PC Technologies.

generally – is retaliation for this criticism.

The document subpoena to Mr. Daugherty demands the following documents:

1. All drafts of the Manuscript that were reviewed by another third party prior to the Manuscript's publication.

2. All comments received on drafts of the Manuscript.

3. All documents related to the source material for drafts of the Manuscript, including documents referenced or quoted in the Manuscript.

4. All promotional materials related to the Manuscript, including, but not limited to, documents posted on social media, commercials featuring you, and presentations or interviews given by you.

The extent to which either party will attempt to use the book in this case is unknown. Regardless of whether the book itself and any of its contents may be relevant – which is not obvious – the relevance of drafts, related promotional materials, or the other materials listed in 1 through 4 above, is not at all apparent. Therefore, the requested materials exceed the scope of permissible discovery.

B.

Finally, Respondent argues that each of the proposed depositions should be barred. According to Respondent, the deponents include current and former employees of Respondent, as well as Respondent's clients and IT service providers.

Respondent first asserts that the testimony will be "duplicative" of information that Complaint Counsel already possesses, and also duplicative of document subpoenas issued to some of the deponents. As noted previously, however, this argument relies on the right or interest of the subpoenaed nonparties not to be burdened with producing duplicative information, which Respondent has no standing to assert in support of a protective order. *See* Section III.B.

Respondent further argues that the depositions are noticed for varying locations across the country, and that the expense that LabMD would expend in defending the depositions "would be astronomical, and outweigh" any benefit. Motion at 10. While Respondent has standing to assert that the depositions would unduly burden Respondent, Respondent fails to submit any evidence to support the claim of "astronomical" costs. "A party seeking to quash a subpoena has the burden of demonstrating that the request is unduly burdensome." *In re Lab. Corp. of Am.*, 2011 FTC LEXIS 31 at *7 (Feb. 28, 2011) (citations omitted). "A movant's general allegation that a subpoena is unduly burdensome is insufficient to carry its burden of showing that the requested discovery should be denied." *In re Lab. Corp. of Am.*, *Id.* at *8 (citations omitted) (finding that nonparty failed to meet its burden that subpoena was unduly burdensome where it provided no specific information regarding the burden or expense involved in producing the requested documents other than its unsupported statement that compliance with the requests

would take months and tens or even hundreds of thousands of dollars).

Moreover, Respondent's assertion that the depositions will take place all over the country is overstated. According to the subpoenas, most of the depositions are set to take place in one location – Atlanta, Georgia – where Respondent is located. In addition, Complaint Counsel asserts that Respondent can reduce its costs by appearing for the depositions telephonically. Opposition at 5. For all the foregoing reasons, Respondent has failed to demonstrate that defending the depositions would be unduly burdensome, as asserted in its Motion.[8]

V.

For all of the above reasons, Respondent's Motion is GRANTED, in part, as to (a) Complaint Counsel's requested discovery into the time period prior to 2005, and (b) Complaint Counsel's requested discovery into drafts, related promotional materials, and other materials listed in Specifications 1-4 of the October 24, 2013 Subpoena *Duces Tecum* issued to Respondent's CEO Michael Daugherty, but is in all other respects DENIED. This Order affects the scope of discovery only and is not a determination, and shall not be construed as a ruling, as to the admissibility of any evidence.

ORDERED:

D. Michael Chappell
Chief Administrative Law Judge

Date: November 22, 2013

[8] Respondent also avers that Mr. Daugherty and Mr. Boyle have already been deposed. Even if these individuals are current employees of Respondent and Respondent has an interest in preventing undue disruption to its operations caused by its employees being occupied with "duplicative" discovery, Respondent fails to support its claim. Moreover, Mr. Daugherty is not among the subpoenaed deponents. Finally, to the extent individuals may have provided sworn testimony during the investigative phase of this case, this would not bar deposing the individuals in connection with this adjudicative phase of the case. *See* 16 C.F.R.§ 3.33(b) ("The fact that a witness testifies at an investigative hearing does not preclude the deposition of that witness"); *In re Polypore Int'l, Inc.*, 2008 FTC LEXIS 155, at *9 ("Simply because the agents of Respondents were examined during the pre-complaint investigation does not preclude Complaint Counsel from taking the depositions of these individuals in accordance with Part III of the Commission's Rules of Practice.").

FOR PUBLICATION

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

FEDERAL TRADE COMMISSION, **Plaintiff,** **v.** **WYNDHAM WORLDWIDE CORPORATION, et al.,** **Defendants.**	**Civil Action No. 13-1887 (ES)** **OPINION**

SALAS, DISTRICT JUDGE

I. INTRODUCTION

The Federal Trade Commission (the "FTC") brought this action under Section 5(a) of the Federal Trade Commission Act (the "FTC Act"), 15 U.S.C. § 45(a), against Wyndham Worldwide Corporation ("Wyndham Worldwide"), Wyndham Hotel Group, LLC ("Hotel Group"), Wyndham Hotels and Resorts, LLC ("Hotels and Resorts"), and Wyndham Hotel Management, Inc. ("Hotel Management") (collectively, "Wyndham" or "Defendants"). The FTC alleges that Wyndham violated Section 5(a)'s prohibition of "acts or practices in or affecting commerce" that are "unfair" or "deceptive."

Specifically, the FTC alleges that Defendants violated both the deception and unfairness prongs of Section 5(a) "in connection with Defendants' failure to maintain reasonable and appropriate data security for consumers' sensitive personal information." (D.E. No. 28, First Amended Complaint for Injunctive and Other Equitable Relief ("Compl.") ¶¶ 1, 44-49). Hotels and Resorts moves to dismiss the FTC's complaint under Federal Rule of Civil Procedure

12(b)(6). (D.E. No. 91-1, Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC ("HR's Mov. Br.") at 6).[1] Its motion to dismiss raises the following three issues.

First, Hotels and Resorts challenges the FTC's authority to assert an unfairness claim in the data-security context. Citing recent data-security legislation and the FTC's public statements, Hotels and Resorts likens this action to *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000). It declares that, under *Brown & Williamson*, the FTC does not have the authority to bring an unfairness claim involving data security. As explained below, however, the Court rejects this challenge to the FTC's authority because the circumstances here differ from those in *Brown & Williamson*.

Second, Hotels and Resorts asserts that the FTC must formally promulgate regulations before bringing its unfairness claim. It contends that, without promulgating such regulations, the FTC violates fair notice principles. But precedent instructs that agencies like the FTC need not formally issue regulations. The Court, therefore, rejects Hotels and Resorts' contention that the FTC must issue regulations before bringing its unfairness claim.

Third, Hotels and Resorts argues that the FTC's allegations are pleaded insufficiently to support either an unfairness or deception claim. Hotels and Resorts asserts that the FTC fails to plead certain elements of each of these claims and fails to otherwise satisfy federal pleading requirements. As detailed below for both the unfairness and deception claims, the Court disagrees.

Having resolved each of these issues in favor of the FTC, the Court DENIES Hotels and Resorts' motion to dismiss.

[1] Wyndham Worldwide, Hotel Group and Hotel Management separately move to dismiss the FTC's complaint, (D.E. No. 92), which the Court will address in a separate opinion. On November 7, 2013, the Court heard oral argument on both motions to dismiss. (*See* D.E. No. 139 ("11/7/13 Tr.")).

II. FACTUAL BACKGROUND[2]

Wyndham Worldwide is in the hospitality business. (Compl. ¶ 7). "At all relevant times," Wyndham Worldwide controlled the acts and practices of the following subsidiaries: Hotel Group, Hotels and Resorts, and Hotel Management. (*Id.* ¶¶ 7-10). Through these three subsidiaries, Wyndham Worldwide "franchises and manages hotels and sells timeshares." (*Id.* ¶ 13).

More specifically, "Hotel Group is a wholly-owned subsidiary of Wyndham Worldwide." (*Id.* ¶ 8). Both Hotels and Resorts and Hotel Management, in turn, are wholly-owned subsidiaries of Hotel Group. (*Id.* ¶¶ 9, 10). Hotels and Resorts licensed the "Wyndham" name to approximately seventy-five independently-owned hotels under *franchise* agreements. (*Id.* ¶ 9). Similarly, Hotel Management licensed the "Wyndham" name to approximately fifteen independently-owned hotels under *management* agreements. (*Id.* ¶ 10).

Under these agreements, Hotels and Resorts and Hotel Management require each Wyndham-branded hotel to purchase—and "configure to their specifications"—a designated computer system that, among other things, handles reservations and payment card transactions. (*Id.* ¶ 15). This system, known as a "property management system," stores consumers' personal information, "including names, addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes." (*Id.*).

The property management systems for *all* Wyndham-branded hotels "are part of Hotels and Resorts' computer network" and "are linked to its corporate network." (*Id.* ¶ 16). Indeed, Hotels and Resorts' computer network "includes its central reservation system" that "coordinates reservations across the Wyndham brand" and, using Hotels and Resorts' website, "consumers

[2] The Court must accept the FTC's factual allegations as true for purposes of resolving Hotels and Resorts' motion to dismiss. *See Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009); *see also Bistrian v. Levi*, 696 F.3d 352, 358 n.1 (3d Cir. 2012) ("As such, we set out facts as they appear in the Complaint and its exhibits.").

can make reservations at any Wyndham-branded hotel." (*Id.* ¶¶ 16, 20). And, although certain Wyndham-branded hotels have their own websites, customers making reservations for these hotels "are directed back to Hotels and Resorts' website to make reservations." (*Id.* ¶ 20).

The FTC alleges that, since at least April 2008, Wyndham "failed to provide reasonable and appropriate security for the personal information collected and maintained by Hotels and Resorts, Hotel Management, and the Wyndham-branded hotels." (*Id.* ¶ 24). The FTC alleges that Wyndham did this "by engaging in a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft." (*Id.*).

As a result of these failures, between April 2008 and January 2010, intruders gained unauthorized access—on three separate occasions—to Hotels and Resorts' computer network, including the Wyndham-branded hotels' property management systems. (*Id.* ¶ 25; *see also id.* ¶¶ 26-39 (detailing the circumstances of the three breaches and impact of each breach)). The intruders "used similar techniques on each occasion to access personal information stored on the Wyndham-branded hotels' property management system servers, including customers' payment card account numbers, expiration dates, and security codes." (*Id.* ¶ 25). And, after discovering the first two breaches, Wyndham "failed to take appropriate steps in a reasonable time frame to prevent the further compromise of Hotels and Resorts' network." (*Id.*).

Wyndham's "failure to implement reasonable and appropriate security measures exposed consumers' personal information to unauthorized access, collection, and use" that "has caused and is likely to cause substantial consumer injury, including financial injury, to consumers and businesses." (*Id.* ¶ 40). Defendants' failure "to implement reasonable and appropriate security measures" caused, for example, the following:

> [T]he three data breaches described above, the compromise of more than 619,000 consumer payment card account numbers, the

> exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss. Consumers and businesses suffered financial injury, including, but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit. Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm.

(*Id.* ¶ 40).

Given these allegations, the FTC brought this action, seeking a permanent injunction to prevent future violations of the FTC Act, as well as certain other relief. (*See id.* at 20-21).

III. LEGAL STANDARD

To withstand a motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Iqbal*, 556 U.S. at 678 (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.*

"When reviewing a motion to dismiss, '[a]ll allegations in the complaint must be accepted as true, and the plaintiff must be given the benefit of every favorable inference to be drawn therefrom.'" *Malleus v. George*, 641 F.3d 560, 563 (3d Cir. 2011) (quoting *Kulwicki v. Dawson*, 969 F.2d 1454, 1462 (3d Cir. 1992)). But the court is not required to accept as true "legal conclusions," and "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Iqbal*, 556 U.S. at 678.

Finally, "[i]n deciding a Rule 12(b)(6) motion, a court must consider only the complaint, exhibits attached to the complaint, matters of the public record, as well as undisputedly authentic

documents if the complainant's claims are based upon these documents." *Mayer v. Belichick*, 605 F.3d 223, 230 (3d Cir. 2010); *see also Buck v. Hampton Twp. Sch. Dist.*, 452 F.3d 256, 260 (3d Cir. 2006) ("In evaluating a motion to dismiss, we may consider documents that are attached to or submitted with the complaint, and any matters incorporated by reference or integral to the claim, items subject to judicial notice, matters of public record, orders, and items appearing in the record of the case.") (internal quotation marks, textual modifications and citations omitted).

IV. DISCUSSION

The Court notes that both the FTC and Hotels and Resorts seem to recognize the importance of data security and the damage caused by data-security breaches. Both also seem to acknowledge that we live in a digital age that is rapidly evolving—and one in which maintaining privacy is, perhaps, an ongoing struggle. And, as evident from the instant action, this climate undoubtedly raises a variety of thorny legal issues that Congress and the courts will continue to grapple with for the foreseeable future.

Hotels and Resorts characterizes this case as the first instance where "the FTC is asking a federal court to hold that Section 5 of the FTC Act—a 1914 statute that prohibits 'unfair and deceptive acts or practices'—authorizes the Commission to regulate the sophisticated technologies that businesses use to protect sensitive consumer information." (HR's Mov. Br. at 1). Hotels and Resorts asserts that the FTC's action "is the Internet equivalent of punishing the local furniture store because it was robbed and its files raided." (*Id.* at 21).

But Hotels and Resorts' motion to dismiss demands that this Court carve out a data-security exception to the FTC's authority and that the FTC publish regulations before filing an unfairness claim in federal court. These demands are, in fact, what bring us into unchartered territory. And, after having wrestled with arguments in the parties' initial briefing, oral

argument, supplemental briefing, as well as in several *amici* submissions, the Court now endeavors to explain why Hotels and Resorts' demands are inconsistent with governing and persuasive authority.[3]

To be sure, the Court does *not* render a decision on liability today. Instead, it resolves a motion to dismiss a complaint. A liability determination is for another day. And this decision does *not* give the FTC a blank check to sustain a lawsuit against every business that has been hacked. Instead, the Court denies a motion to dismiss given the allegations in *this* complaint—which must be taken as true at this stage—in view of binding and persuasive precedent.

A. The FTC's Unfairness Claim (Count Two)

Hotels and Resorts first challenges the FTC's unfairness claim. (HR's Mov. Br. at 7). Under this claim, the FTC alleges that "Defendants have failed to employ reasonable and appropriate measures to protect personal information against unauthorized access." (Compl. ¶ 47). The FTC alleges that "Defendants' actions caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition" and, therefore, "Defendants' acts and practices . . . constitute unfair acts or practices" under Section 5 of the FTC Act. (*Id.* ¶¶ 48-49).

1. Whether *Brown & Williamson* preempts the FTC's authority over data security

a. <u>The parties' contentions</u>

Hotels and Resorts analogizes this action to *Brown & Williamson*, arguing that the FTC's unfairness authority does not cover data security. (HR's Mov. Br. at 7-8, 14). Hotels and

[3] The Court previously granted leave for the following entities to file brief *amici curiae*: the International Franchise Association, (D.E. No. 119); the Chamber of Commerce of the United States of America, Retail Litigation Center, American Hotel & Lodging Association, and National Federation of Independent Business, (D.E. No. 120); TechFreedom, International Center for Law & Economics, and Consumer Protection Scholars Justin Hurwitz, Todd J. Zywicki, and Paul Rubin, (D.E. No. 121); and Public Citizen, Inc. and Chris Jay Hoofnagle, (D.E. No. 122). The Court has considered these submissions and appreciates these entities' assistance in resolving Hotels and Resorts' motion.

Resorts argues that Congress has, in fact, settled on "a less extensive regulatory scheme" and passed narrowly tailored data-security legislation, indicating that these later-enacted laws "shape or focus" the meaning of Section 5. (*Id.* at 10, 14 (quoting *Brown & Williamson*, 529 U.S. at 143, 148)). Hotels and Resorts contends that this "overall statutory landscape" does not authorize the FTC to generally establish data-security standards for the private sector under Section 5. (*Id.* at 7-8).

Specifically, Hotels and Resorts identifies several statutes that purportedly authorize "particular federal agencies to establish minimum data-security standards in narrow sectors of the economy," including: the Fair Credit Reporting Act ("FCRA"); the Gramm-Leach-Bliley Act ("GLBA"); the Children's Online Privacy Protection Act ("COPPA"); and the Health Insurance Portability and Accountability Act of 1996 ("HIPPA"). (*Id.* at 9, 9 n.1 (discussing statutes and citing respective statutory codifications)).[4]

Hotels and Resorts also references pending legislation, namely the Cyber Intelligence Sharing and Protection Act ("CISPA"), arguing that this would "abandon[] any attempt to create comprehensive cybersecurity performance requirements" and is "irreconcilable" with the FTC's data-security regulation since this legislation would exempt liability in certain circumstances. (*Id.* at 12-13).

Hotels and Resorts further argues that, like the FDA's disclaimers over tobacco regulation in *Brown & Williamson*, the FTC has disclaimed authority to regulate data security under Section 5's unfairness prong and, in fact, has asked Congress to give it the very authority it "purports to wield in this case." (*Id.* at 10-11, 14). And Hotels and Resorts contends that, in view of the economic and political considerations associated with data security, "it defies

[4] Hotels and Resorts asserts that Congress's "targeted grants of authority would make no sense if Section 5 already gave the FTC authority to regulate data security in *all* circumstances." (D.E. No. 152-1, Joint Supplemental Letter Brief ("Jnt. Supp. Br.") at 1 (citing the FCRA, GLBA, and COPPA)).

common sense to think that Congress would have delegated [this] responsibility to the FTC." (*Id.* at 12-13 (citing *Brown & Williamson*, 529 U.S. at 133, 160)). In sum, Hotels and Resorts declares that "[t]here is no stronger basis for the FTC to claim authority to regulate data-security in this case than there was for the FDA to claim authority to regulate tobacco in *Brown & Williamson*." (*Id.* at 14).

In opposition, the FTC argues that *Brown & Williamson* is distinguishable. (D.E. No. 110, Plaintiff's Response in Opposition to the Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC ("FTC's Opp. Br.") at 10). The FTC insists that, unlike *Brown & Williamson*, its own assertion of authority here would not result in any statutory inconsistencies. (*Id.*).

The FTC argues that, in actuality, Hotels and Resorts cites statutes that supplement the FTC's Section 5 authority for three reasons: (1) those statutes do not have the "consumer injury" requirement that Section 5 has; (2) they grant the FTC additional powers that it otherwise lacks; and (3) they "affirmatively compel (rather than merely authorize) the FTC to use its consumer-protection authority in specified ways." (Jnt. Supp. Br at 6; *see also* FTC's Opp. Br. at 16 n.4 ("The liability exemption provision [in CISPA] is expressly limited to potential liability from complying with that Act.")).[5] Indeed, the FTC avers that Congress purposely gave it broad power under Section 5 of the FTC Act and that its decision to enforce the FTC Act in the data-security context is entitled to deference. (FTC's Opp. Br. at 11).

Moreover, the FTC argues that, unlike the FDA's repeated denials of authority over tobacco in *Brown & Williamson*, the FTC has never disavowed authority over unfair practices

[5] In its opposition brief, the FTC argued that the subsequent data-security laws "enhance FTC authority with new legal tools" such as "rulemaking and/or civil penalty authority." (FTC's Opp. Br. at 12). At oral argument, however, the FTC seemed to reconcile these data-security laws by arguing that Section 5 requires "substantial injury," whereas these other laws do not. (*See* 11/7/13 Tr. at 44:17-45:22). To provide the parties a full and fair opportunity to present their arguments, as well as provide any updates on recent developments, the Court invited supplemental briefing. (*See* D.E. Nos. 146, 152, 153, 156 and 158). The Court has considered all of these submissions in resolving Hotels and Resorts' motion to dismiss.

related to data security. (*Id.* at 10, 13). Lastly, the FTC proclaims that "any question about the FTC's authority in the data security area is put to rest by the *LabMD* decision"—a recent decision by the FTC in an administrative action that the FTC contends deserves deference under *Chevron, U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984). (Jnt. Supp. Br. at 6, 8-9).

b. Analysis

The Court rejects Hotels and Resorts' invitation to carve out a data-security exception to the FTC's unfairness authority because this case is different from *Brown & Williamson*. In *Brown & Williamson*, the Supreme Court determined that, "[c]onsidering the [Food, Drug, and Cosmetic Act ("FDCA")] as a whole, it is clear that Congress intended to exclude tobacco products from the FDA's jurisdiction." 529 U.S. at 142. It reasoned that "if tobacco products were within the FDA's jurisdiction, the Act would require the FDA to remove them from the market entirely." *Id.* at 142. But, the Court determined that this "would *contradict* Congress'[s] clear intent as expressed in its more recent, tobacco-specific legislation" in which it "foreclosed the removal of tobacco products from the market." *Id.* at 137, 143 (emphasis added). The Supreme Court explained that "Congress, for better or for worse, has created a distinct regulatory scheme for tobacco products, squarely rejected proposals to give the FDA jurisdiction over tobacco, and repeatedly acted to *preclude* any agency from exercising significant policymaking authority in the area." *Id.* at 159-60 (emphasis added).

But no such dilemma exists here. Hotels and Resorts fails to explain how the FTC's unfairness authority over data security would lead to a result that is incompatible with more recent legislation and thus would "plainly *contradict* congressional policy." *See Brown & Williamson*, 529 U.S. at 139 (emphasis added); *see also Massachusetts v. EPA*, 549 U.S. 497,

531 (2007) (distinguishing *Brown & Williamson*, finding that the "EPA has not identified any congressional action that *conflicts* in any way with the regulation of greenhouse gases from new motor vehicles") (emphasis added). Instead, Hotels and Resorts unequivocally recognizes that "the FCRA, GLBA, and COPPA all contain detailed provisions granting the FTC *substantive* authority over data-security practices." (Jnt. Supp. Br at 2-3).

To be sure, Hotels and Resorts contends that these statutes are "entirely superfluous" if the FTC "already possess[ed] generalized data-security authority under Section 5." (D.E. No. 156, HR's Reply to the Parties' Joint Supplemental Letter Brief ("HR's Reply to Jnt. Supp. Br.") at 2). In fact, Hotels and Resorts posits that "the FTC must prove substantial, unavoidable consumer injury as part of enforcing those statutes" and that "no provision of the FCRA, GLBA, or COPPA purports to relieve the FTC of its duty to prove substantial consumer injury." (Jnt. Supp. Br at 3). In Hotels and Resorts' view, if "both sets of statutes require substantial consumer injury," then "the FTC's understanding of Section 5 cannot be sustained without rendering the terms of the FCRA, GLBA, and COPPA entirely superfluous." (*Id.*).

But this ignores the critical premise of *Brown & Williamson*. *See, e.g.*, 529 U.S. at 133 ("[W]e find that Congress has directly spoken to the issue here and *precluded* the FDA's jurisdiction to regulate tobacco products.") (emphasis added). Here, subsequent data-security legislation seems to complement—*not preclude*—the FTC's authority.

Specifically, the FTC Act defines "unfair acts or practices" as those that "cause[] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). And Hotels and Resorts identifies statutes, such as the FCRA,

GLBA, and COPPA, that each set forth different standards for injury in certain delineated circumstances, granting the FTC *additional* enforcement tools.[6]

Thus, unlike the FDA's regulation over tobacco, the FTC's unfairness authority over data security can coexist with the existing data-security regulatory scheme. *See Brown & Williamson*, 529 U.S. at 143 ("[I]f tobacco products were within the FDA's jurisdiction, the Act would require the FDA to remove them from the market entirely. But a ban would contradict Congress'[s] clear intent as expressed in its more recent, tobacco-specific legislation. The inescapable conclusion is that *there is no room for tobacco products within the FDCA's regulatory scheme*.") (emphasis added). No such "inescapable conclusion" exists here. *See id.*

Moreover, in *Brown & Williamson*, Congress's tobacco-specific legislation "creat[ed] a distinct regulatory scheme" that was enacted "against the background of the FDA repeatedly and consistently asserting that it lacks jurisdiction under the FDCA to regulate tobacco products as customarily marketed." *Id.* at 155-56. In fact, the FDA's assertion to regulate tobacco was "[c]ontrary to its representations to Congress since 1914." *Id.* at 159. Thus, Congress ratified the "FDA's *plain and resolute position* that the FDCA gives the agency *no authority to regulate* tobacco products as customarily marketed." *Id.* (emphasis added).

Here, however, the FTC representations identified by Hotels and Resorts do not amount to an analogous position that would, as a matter of law, support precluding the FTC from bringing any enforcement action in the data-security context. Specifically, Hotels and Resorts seems to rely on the following three representations that purportedly show the FTC disclaiming authority over data security:

[6] Notably, the FTC contends that "Section 45(n) places limitations on the Commission's authority to declare particular actions unfair under Section 5[] either in litigation or rulemaking" and that "[i]t has no application where Congress itself has statutorily defined categories of actions to be unlawful and authorized the FTC to enforce those statutes." (Jnt. Supp. Br. at 7 n.1). Although it had an opportunity do so, Hotels and Resorts revealingly leaves this contention unrebutted. (*See generally* HR's Reply to Jnt. Supp. Br. at 3).

- "Currently, the Commission has limited authority to prevent abusive practices in this area. The Federal Trade Commission Act (the 'FTC Act'), 15 U.S.C. §§ 41 *et seq.*, grants the Commission authority to seek relief for violations of the Act's prohibitions on unfair and deceptive practices in and affecting commerce, an authority limited in this context to ensuring that Web sites follow their stated information practices." *Consumer Privacy on the World Wide Web*, Hearing before H. Comm. on Commerce, Subcomm. on Telecomm., 105th Cong., at n.23 (July 21, 1998) (Chairman Robert Pitofsky proposing that, under new legislation, "[w]eb sites would be required to take reasonable steps to protect the security and integrity" of "personal identifying information from or about consumers" collected "online");

- "The Commission's authority over the collection and dissemination of personal data collected online stems from Section 5 of the Federal Trade Commission Act (the 'FTC Act' or 'Act'), and the Children's Online Privacy Protection Act ('COPPA') . . . . As a general matter, however, the Commission lacks authority to require firms to adopt information practice policies or to abide by the fair information practice principles on their Web sites, or portions of their Web sites, not directed to children." FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, at 33-34 (2000);

- "The agency's jurisdiction is (over) deception . . . If a practice isn't deceptive, we can't prohibit them from collecting information. The agency doesn't have the jurisdiction to enforce privacy. It has the authority to challenge deceptive practices." Jeffrey Benner, *FTC Powerless to Protect Privacy*, Wired, May 31, 2001 (quoting Lee Peeler, former Associate Director of Advertising Practices at the FTC).

(11/7/13 Tr. at 19:22-21:5, 24:5-26:4; HR's Mov. Br. at 10-11).[7]

But the Court is not convinced that these statements, made within a three-year period, equate to a resolute, unequivocal position under *Brown & Williamson* that the FTC has *no* authority to bring *any* unfairness claim involving data security. *See* 529 U.S. at 156-59. In fact, as Hotels and Resorts must concede, the FTC brought unfairness claims in the data-security context shortly after these representations. (*See* 11/7/13 Tr. at 25:20-24, 74:9-12 (presenting timeline of events showing the FTC bringing unfairness claims in the data-security context in 2005)). And the FTC's subsequent representations confirm its authority in this arena, not deny it. *See, e.g.*, *Identity Theft: Innovative Solutions for an Evolving Problem: Hearing before the*

[7] For the reader's convenience and simplicity's sake, the Court reproduces portions of the FTC's representations and the related citations from Hotels and Resorts' briefing and presentation at oral argument.

Subcomm. on Terrorism, Tech. & Homeland Sec. of the S. Comm. on the Judiciary, 110th Cong. at 5-6 (Mar. 21, 2007).

Although Hotels and Resorts reasonably contends that the "digital age is moving much more quickly [such that] the timeframe here is compressed," the public record here is unlike the lengthy, forceful history of repeated and consistent disavowals in *Brown & Williamson*. Thus, even accepting that the FTC shifted its stance on data security, this cannot limit its authority without more. *See Brown & Williamson*, 529 U.S. at 156-57 ("Certainly, an agency's initial interpretation of a statute that it is charged with administering is not 'carved in stone.'").

Notably, Hotels and Resorts avers that the FTC never indicated that it *did* have unfairness authority over data security in the three-year period that Hotels and Resorts relies upon:

> Where is there any where from 1998 to 2001 where the FTC is telling Congress or even the Executive Branch, that [it has] this authority, so there is no need to do anything? There is nowhere. . . . I would submit the FTC actually doesn't have anything where they go to Congress and in 2000 say we have this authority. There is nothing you need to do.

(11/7/13 Tr. at 26:9-17).

Tellingly, however, Hotels and Resorts fails to explain how this is a relevant consideration under *Brown & Williamson*. Said differently, Hotels and Resorts analogizes this case to *Brown & Williamson*—but fails to explain how *Brown & Williamson* requires a federal agency to *affirm* its authority before asserting it.

Thus, although "subsequent acts can shape or focus" a range of "plausible meanings" that a statute may have, the data-security legislation and the FTC's representations cited by Hotels and Resorts do not call for a data-security exception to the FTC's unfairness authority. *See Brown & Williamson*, 529 U.S. at 143. After all, *Brown & Williamson* was "hardly an ordinary case" because, "[t]o find that the FDA has the authority to regulate tobacco products, one must

not only adopt an extremely strained understanding of 'safety' as it is used throughout the Act—a concept central to the FDCA's regulatory scheme—but also ignore the plain implication of Congress'[s] subsequent tobacco-specific legislation." 529 U.S. at 159-60.

To be sure, the Court's analysis herein does not simply rest on how "important, conspicuous, and controversial" data security is. *See Brown & Williamson*, 529 U.S. at 161. Undoubtedly, "an administrative agency's power to regulate in the public interest must always be grounded in a valid grant of authority from Congress." *Id.*

And, to that end, the Court is guided by precedent that compels rejecting Hotels and Resorts' request to carve out a data-security exception to the FTC's authority. *See, e.g.*, *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239-40 (1972) ("When Congress created the Federal Trade Commission in 1914 and charted its power and responsibility under [Section] 5, it explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' by tying the concept of unfairness to a common-law or statutory standard or by enumerating the particular practices to which it was intended to apply." (citing S. Rep. No. 597, at 13 (1914))); *Am. Fin. Servs. Ass'n v. FTC*, 767 F.2d 957, 967 (D.C. Cir. 1985) ("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.").[8]

2. Whether the FTC must promulgate rules and regulations to satisfy fair notice principles

a. <u>The parties' contentions</u>

Hotels and Resorts argues that, even if Section 5 gives the FTC sufficient authority, "it would violate basic principles of fair notice and due process to hold [Hotels and Resorts] liable

[8] The parties vigorously dispute whether a recent FTC administrative adjudication—*LabMD, Inc.*, 2014 WL 253518 (2014) (unanimous commission review)—is entitled to *Chevron* deference. (*See* Jnt. Supp. Br. at 6; HR's Reply to Jnt. Supp. Br. at 1-2). But, even without deferring to the agency's interpretation of Section 5 in *LabMD*, the Court finds that *Brown & Williamson* is distinguishable and thus need not resolve this deference issue.

in this case" without "rules, regulations, or other guidelines explaining what data-security practices the Commission believes Section 5 to forbid or require." (HR's Mov. Br. at 15). Hotels and Resorts contends that the FTC's "failure to publish any interpretive guidance whatsoever" violates fair notice principles and "bedrock principles of administrative law." (Jnt. Supp. Br. at 4 (citing *FCC v. Fox Television Stations, Inc.*, 132 S. Ct. 2307, 2317 (2012) and *Sec'y of Labor v. Beverly Healthcare-Hillview*, 541 F.3d 193, 202 (3d Cir. 2008))).

Hotels and Resorts further asserts that, generally, agencies cannot rely on enforcement actions to make new rules and concurrently hold a party liable for violating the new rule. (HR's Mov. Br. at 15). Indeed, Hotels and Resorts avers that, to do so, the agency must have previously set forth with *ascertainable certainty* the standards it expects private parties to obey—but that the FTC's mere reasonableness standard provides no such guidance "in the highly complex and sophisticated world of data security." (D.E. No. 115, Reply in Support of Motion to Dismiss by Defendant Wyndham Hotels & Resorts LLC ("HR's Reply Br.") at 5-6 (citing *Dravo Corp. v. Occupational Safety & Health Review Comm'n*, 613 F.2d 1227, 1233 (3d Cir. 1980))). Hotels and Resorts adds that the FTC's prior consent decrees and its business guidance brochure provide no such guidance. (*Id.* at 6-7; Jnt. Supp. Br. at 5 ("[C]onsent decrees do not constrain FTC discretion and thus cannot provide any meaningful notice to third parties. . . . And the informal brochure on which the FTC so heavily relies . . . is far too vague to provide meaningful guidance, particularly in the complex world of data security.") (citations omitted)).

Hotels and Resorts argues that, moreover, the FTC "can proceed by adjudication only if it has already provided the baseline level of fair notice that the Constitution requires"—and that the FTC has not done so here. (HR's Reply to Jnt. Supp. Br. at 3). Hotels and Resorts accordingly argues that, since neither the FTC nor Section 5 itself provides "fair notice," the Court should

dismiss the instant action. (HR's Mov. Br. at 17; *see also* HR's Reply Br. at 4 ("Section 5 also does not permit the FTC to bring data-security enforcement actions without first publishing rules or regulations explaining in advance what parties must do to comply with the law." (citing Gerard M. Stegmaier & Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 Geo. Mason L. Rev. 673 (2013)))).

In response, the FTC argues that, in the data-security context, "reasonableness is the touchstone" and that "unreasonable data security practices are unfair." (FTC's Opp. Br. at 17). The FTC contends that the Court can evaluate the reasonableness of Hotels and Resorts' data-security program in view of the following guidance: (1) industry guidance sources that Hotels and Resorts itself seems to measure its own data-security practices against; and (2) the FTC's business guidance brochure and consent orders from previous FTC enforcement actions. (*Id.* at 17-20).

The FTC also asserts that data-security standards can be enforced in an industry-specific, case-by-case manner and, further, that it has the discretion to enforce the FTC Act's prohibition of unfair practices through individual enforcement action rather than rulemaking. (*Id.* at 20, 22). And it argues that the "ascertainable certainty" standard does not apply—but that even if it did, reasonableness provides ascertainable certainty to companies. (11/7/13 Tr. at 74:7-19, 153:1-6; Jnt. Supp. Br. at 9 n.2).

Indeed, the FTC analogizes its enforcement action here to other circumstances where agencies bring actions without "particularized prohibitions," such as those involving the National Labor Relations Board ("NLRB") and the Occupational Safety and Health Act ("OSHA"). (FTC's Opp. Br. at 23). In short, the FTC argues that fair notice does *not* necessarily require issuing regulations—and that accepting Hotels and Resorts' argument "would undermine 100

years of FTC precedent" because "the FTC could never protect consumers from unfair practices without first issuing a regulation governing the specific practice at issue." (Jnt. Supp. Br. at 9).

b. Analysis

"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." *Fox Television Stations, Inc.*, 132 S. Ct. at 2317. At times, Hotels and Resorts seems to improperly characterizes the issue as being whether the FTC must provide any fair notice at all. (*See* HR's Reply to Jnt. Supp. Br. at 3 ("The FTC's primary response is that it is not obligated to provide any fair notice at all . . . .")). But this is not the issue. Instead, the issue is whether fair notice *requires* the FTC to formally issue rules and regulations before it can file an unfairness claim in federal district court. And, to that extent, the Court is not so persuaded.

"[W]here an agency . . . is given an option to proceed by rulemaking or by individual adjudication the choice is one that lies in the informed discretion of the administrative agency." *PBW Stock Exch., Inc. v. SEC*, 485 F.2d 718, 732 (3d Cir. 1973) (citing *NLRB v. Wyman-Gordon Co.*, 394 U.S. 759, 772 (1969) (Black, J., concurring); *SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947)). After all, "problems may arise in a case which the administrat[ive] agency could not reasonably foresee" or "the agency may not have had sufficient experience with a particular problem to warrant rigidifying its tentative judgment into a hard and fast rule" or "the problem may be so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule." *Chenery*, 332 U.S. at 202-03; s*ee also Am. Gas Ass'n v. FERC*, 912 F.2d 1496, 1519 (D.C. Cir. 1990) ("[A]gency discretion is at its peak in deciding such matters as whether to address an issue by rulemaking or adjudication. The Commission seems on especially

solid ground in choosing an individualized process where important factors may vary radically from case to case.") (citations omitted).[9]

Indeed, "the proscriptions in [Section] 5 are flexible, to be defined with particularity by the myriad of cases from the field of business." *FTC v. Colgate-Palmolive Co.*, 380 U.S. 374, 385 (1965) (internal quotation marks omitted) (explaining that "[t]his statutory scheme necessarily gives the Commission an influential role in interpreting [Section] 5 and in applying it to the facts of particular cases arising out of unprecedented situations"); *see also Sperry & Hutchinson*, 405 U.S. at 239-40.

Accordingly, Circuit Courts of Appeal have affirmed FTC unfairness actions in a variety of contexts *without* preexisting rules or regulations specifically addressing the conduct-at-issue. *See, e.g., FTC v. Neovi, Inc.*, 604 F.3d 1150, 1153, 1155-59 (9th Cir. 2010) (affirming summary judgment in favor of the FTC for violation of Section 5's unfairness prong where website "created and delivered unverified checks at the direction of registered users" and "fraudsters and con artists extensively abused the website"); *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1191, 1193-95 (10th Cir. 2009) (affirming summary judgment in favor of the FTC for violation of Section 5's unfairness prong where website sold personal data, explaining that "conduct may constitute an unfair practice under § 5(a) of the FTCA even if it is not otherwise unlawful").

Hotels and Resorts insists that an agency "has the responsibility to state with ascertainable certainty what is meant by the standards [it] has promulgated." *Dravo Corp.*, 613 F.2d at 1232-33 (quoting *Diamond Roofing Co. v. Occupational Safety & Health Review*

[9] *See also FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 520 (2009) ("[T]he agency's decision to consider the patent offensiveness of isolated expletives on a case-by-case basis is not arbitrary or capricious."); *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 294 (1974) ("It is doubtful whether any generalized standard could be framed which would have more than marginal utility. The Board thus has reason to proceed with caution, developing its standards in a case-by-case manner with attention to the specific character of the buyers' authority and duties in each company.").

Comm'n, 528 F.2d 645, 649-50 (5th Cir. 1976)). Indeed, "ascertainable certainty" is the "applicable standard for fair notice." *Sec'y of Labor v. Beverly Healthcare-Hillview*, 541 F.3d 193, 202 (3d Cir. 2008).

Correspondingly, Hotels and Resorts asserts that "*Beverly* holds that the 'ascertainable certainty' standard applies," but that "Section 5 contains nothing but generalized, vague language, and the FTC has failed to remedy that vagueness by 'provid[ing] a sufficient, publicly accessible statement' of what the statute requires." (HR's Reply to Jnt. Supp. Br. at 4 (quoting *Beverly Healthcare-Hillview*, 541 F.3d at 202)).

But this does not mean that any ambiguity in a regulation prevents punishment. *Beverly Healthcare-Hillview*, 541 F.3d at 202. Instead, the "ascertainable certainty" standard applies when:

> (1) the agency had given conflicting public interpretations of the regulation, or, (2) the regulation is so vague that the ambiguity can only be resolved by deferring to the agency's own interpretation of the regulation (i.e., a situation in which the ambiguity is resolved by something comparable to a step-two analysis under *Chevron*), and the agency has failed to provide a sufficient, publicly accessible statement of that interpretation before the conduct in question.

Id. (quoting *United States v. Lachman*, 387 F.3d 42, 57 (1st Cir. 2004)).

The parties strongly contest whether the ascertainable certainty standard applies. (*See* Jnt. Supp. Br. at 4, 9 n.2; HR's Reply to Jnt. Supp. Br. at 4). Notwithstanding this dispute, however, Hotels and Resorts' arguments boil down to one proposition: the FTC cannot bring an enforcement action under Section 5's unfairness prong without first formally publishing rules and regulations. And Hotels and Resorts does *not* limit this to the data-security context.[10] But

[10] At oral argument, for instance, the FTC argued that Hotels and Resorts demands that, "for every unfairness case that the FTC brings, there must first be a rule" and that the FTC did not "think the argument was just on data-security cases," but "all unfairness cases." (11/7/13 Tr. at 99:3-7). Hotels and Resorts did not contest this argument.

accepting Hotels and Resorts' proposition would necessarily require the Court to sidestep long-standing precedent, detailed above, that suggests precisely the opposite—i.e., that the FTC does *not* necessarily need to formally publish rules and regulations since the proscriptions in Section 5 are necessarily flexible.

To be sure, the Court finds that neither *Dravo* nor *Beverly* requires the FTC to formally publish a regulation before bringing an enforcement action under Section 5's unfairness prong. Indeed, the Third Circuit has affirmed that "it is within the [agency's] discretion whether to proceed between ad hoc litigation or regulation." *Voegele Co. v. Occupational Safety & Health Review Comm'n*, 625 F.2d 1075, 1079 (3d Cir. 1980); *see also PBW Stock Exch.*, 485 F.2d at 732 ("The courts have consistently held that where an agency, as in this case, is given an option to proceed by rulemaking or by individual adjudication the choice is one that lies in the informed discretion of the administrative agency.").

Undoubtedly, "laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *Fox Television Stations*, 132 S. Ct. at 2317; *see also Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2168 (2012) ("It is one thing to expect regulated parties to conform their conduct to an agency's interpretations once the agency announces them; it is quite another to require regulated parties to divine the agency's interpretations in advance or else be held liable when the agency announces its interpretations for the first time in an enforcement proceeding and demands deference."); *Fabi Constr. Co. v. Sec'y of Labor*, 508 F.3d 1077, 1088 (D.C. Cir. 2007) ("Even if the Secretary's interpretation were reasonable, announcing it for the first time in the context of this adjudication deprives Petitioners of fair notice. Where, as here, a party first receives actual notice of a proscribed activity through a

---

Indeed, Hotels and Resorts predicts that the Third Circuit will order the FTC to "go back and publish a regulation" since it is "an agency with rule[-]making authority." (*Id.* at 91:23-92:8).

citation, it implicates the Due Process Clause of the Fifth Amendment."); *Gen. Elec. Co. v. EPA*, 53 F.3d 1324, 1328-29 (D.C. Cir. 1995) ("In the absence of notice—for example, where the regulation is not sufficiently clear to warn a party about what is expected of it—an agency may not deprive a party of property by imposing civil or criminal liability."). Hotels and Resorts uses these precepts to argue that the FTC must issue regulations—or else an FTC unfairness claim must be dismissed.

But the Court is unpersuaded that regulations are the *only* means of providing sufficient fair notice. Indeed, Section 5 codifies a three-part test that proscribes whether an act is "unfair." *See* 15 U.S.C. § 45(n). And, notably, Hotels and Resorts' only response to the FTC's analogy to tort liability—where liability is routinely found for unreasonable conduct *without* the need for particularized prohibitions—is the following: "While the negligence standard has long been a cornerstone of tort law, no Article III court has *ever—not once*—articulated the data-security standards that Section 5 of the FTC Act supposedly imposes on regulated parties." (HR's Reply to Jnt. Supp. Br. at 5). The Court is not persuaded by this argument that essentially amounts to: since no court has, no court can—especially since Hotels and Resorts itself recognizes how "quickly" the digital age and data-security world is moving. (*See* 11/7/13 Tr. at 25:12-14).

Furthermore, agencies in other circumstances can bring enforcement actions without issuing the particularized prohibitions that Hotels and Resorts demands here. *See* 29 U.S.C. § 158(d) (proscribing the NLRB's requirement that "to bargain collectively is the performance of the mutual obligation of the employer and the representative of the employees to meet at reasonable times and confer in *good faith* with respect to wages, hours, and other terms and conditions of employment") (emphasis added); 29 U.S.C. § 654 (requiring, under OSHA, that each employer must "furnish to each of his employees employment and a place of employment

which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees").

Again, given the rapidly-evolving nature of data security, the Court is not persuaded by Hotels and Resorts' attempt to undermine the FTC's analogies involving the National Labor Relations Act and OSHA on the grounds that precedent is lacking. (*See* HR's Reply Br. at 7 ("Unlike data-security regulation under Section 5, the duty to negotiate in good faith has a long-established meaning in contract law. . . . Similarly, there are over 30 years of concrete, specific agency guidelines specifying the obligations imposed by the General Duty Clause.") (citation omitted)).

And, that the Department of Homeland Security and the National Institute of Standards and Technology have purportedly "managed" to "craft generalized data-security rules" is inapposite to the issue here. (*See* Jnt. Supp. Br. at 4). Hotels and Resorts argues that, since these agencies have issued such rules, the FTC "can certainly do the same." (*Id.* at 5). In other words, Hotels and Resorts argues that, because the FTC has the power to issue particularized regulations and that it is plausible to do so, it *must*. (*See id.*; 11/7/13 Tr. at 87:20-88:1 ("I think it is black letter law that an agency with rule-making authority, which they have, they have rule-making authority, Congress has given it to them, that when they are going to take action, enforcement actions, they have to publish rules in order to give companies fair notice of what is prohibited by their actions.")).

But the contour of an unfairness claim in the data-security context, like any other, is necessarily "flexible" such that the FTC can apply Section 5 "to the facts of particular cases arising out of unprecedented situations." *See Colgate-Palmolive Co.*, 380 U.S. at 384-85. And, Hotels and Resorts invites this Court to dismiss the FTC's complaint on fair notice grounds

despite the FTC's many public complaints and consent agreements, as well as its public statements and business guidance brochure—and despite Hotels and Resorts' *own* references to "industry standard practices" and "commercially reasonable efforts" in its privacy policy. (*See* Compl. ¶ 21).[11]

The Court declines to do so. *See FTC v. R.F. Keppel & Bro.*, 291 U.S. 304, 310 n.1 (1934) ("It is believed that the term 'unfair competition' has a legal significance which can be enforced by the commission and the courts, and that it is no more difficult to determine what is unfair competition than it is to determine what is a reasonable rate or what is an unjust discrimination."); *Voegele*, 625 F.2d at 1077-78 (affirming that the disputed language in an OSHA regulation implied "an objective standard[,] the reasonably prudent person test," which is not unconstitutionally vague).

Indeed, "the rulings, interpretations and opinions of the Administrator under this Act, while not controlling upon the courts by reason of their authority, do constitute a body of experience and informed judgment *to which courts and litigants may properly resort for guidance*." *Gen. Elec. Co. v. Gilbert*, 429 U.S. 125, 141-42 (1976) (emphasis added) (internal quotation marks omitted), *superseded by statute on other grounds*, Pregnancy Discrimination Act, 42 U.S.C. § 2000e-(k). Hotels and Resorts' argument that consent orders do not carry the force of law, therefore, misses the mark.[12]

---

[11] *See, e.g.*, Protecting Personal Information: A Guide for Business (2007), http://business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf. The FTC also cites its various administrative complaints and consent orders—the public accessibility of which are not contested by Hotels and Resorts. (*See* FTC's Opp. Br. at 19; HR's Reply Br. at 6).

[12] Hotels and Resorts asserts that "[s]tatements that do not constrain governmental authority do not provide the fair notice that due process requires." (HR's Reply Br. at 7 (citing *City of Chicago v. Morales*, 527 U.S. 41, 63-64 (1999)). The Court finds Hotels and Resorts' reliance on *Morales* unconvincing. *See* 527 U.S. at 63-64 ("That the police have adopted *internal* rules limiting their enforcement to certain designated areas in the city would not provide a defense to a loiterer who might be arrested elsewhere. Nor could a person who knowingly loitered with a well-known gang member anywhere in the city safely assume that they would not be ordered to disperse no matter how innocent and harmless their loitering might be.") (emphasis added).

Finally, the Court is not convinced that this outcome affirms Section 5's vagueness such that "FTC data-security actions . . . would be exempted from Rule 12(b)(6) scrutiny," as Hotels and Resorts contends. (*See* HR's Reply Br. at 8). This position ignores that, in addition to various sources of guidance for measuring reasonableness, a statutorily-defined standard exists for asserting an unfairness claim. *See* 15 U.S.C. § 45(n). Moreover, the Court must consider the untenable consequence of accepting Hotels and Resorts' proposal: the FTC would have to cease bringing *all* unfairness actions without first proscribing particularized prohibitions—a result that is in direct contradiction with the flexibility necessarily inherent in Section 5 of the FTC Act.

3. Whether the FTC alleges substantial, unavoidable consumer injury and otherwise satisfies federal pleadings requirements

a. <u>The parties' contentions</u>

Hotels and Resorts proclaims that an unfair practice must, by statute, cause or be likely to cause "*substantial injury to consumers* which is *not reasonably avoidable* by consumers themselves"—but that consumer injury from theft of payment card data is never substantial and always avoidable. (HR's Mov. Br. at 19 (quoting 15 U.S.C. § 45(a))).

More specifically, Hotels and Resorts contends that federal law places a $50 limit on consumer liability for unauthorized use of a payment card and that all major credit card brands waive liability for even this small amount. (*Id.*). And Hotels and Resorts contends that consumers can have their issuer rescind any unauthorized charges. (*Id.*). Hotels and Resorts argues that consumers, therefore, cannot suffer any "substantial injury" from the breaches that were not reasonably avoidable. (*Id.* at 19-20). Hotels and Resorts adds that any "incidental injuries that consumers suffered," such as monitoring financial information, is insufficient. (*Id.* at 20-21 (citing *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011))).

Finally, Hotels and Resorts asserts that the FTC's complaint fails "basic pleading requirements" because the FTC alleges "legal conclusions couched as factual allegations" and fails to adequately plead causation. (*Id.* at 22-23). As to causation specifically, Hotels and Resorts argues that the FTC does not allege "*how* the alleged data-security failures caused the intrusions, or *how* the intrusions resulted in any particular consumer harm." (*Id.* at 23).

In opposition, the FTC argues that its complaint pleads sufficient facts to support an unfairness claim involving data-security practices as follows: (1) that substantial injury resulted from Hotels and Resorts' unreasonable data-security practices; (2) this injury was not reasonably avoidable by consumers; (3) Hotels and Resorts' practices caused this injury; and (4) Hotels and Resorts' practices were unreasonable and there were no countervailing benefits to Hotels and Resorts' failure to address its data-security flaws. (FTC's Opp. Br. at 3-4).

b. Analysis

The Court finds that the FTC's complaint sufficiently pleads an unfairness claim under the FTC Act and satisfies Federal Rule of Civil Procedure 8(a). An act or practice is unfair if it (1) "causes or is likely to cause substantial injury to consumers," (2) "which is not reasonably avoidable by consumers themselves," and (3) is "not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n). Hotels and Resorts challenges the FTC's allegations as to the first two elements of this standard, as well as the FTC's purported use of "conclusory standards." (*See* HR's Mov. Br. at 19, 22; 11/7/13 Tr. at 129:7-13). The Court accordingly addresses each of Hotels and Resorts' three contentions.

i. *"Substantial injury" and causation allegations*

First, the FTC adequately pleads "substantial injury to consumers" and that Hotels and Resorts' practices caused this injury. It pleads, in relevant part, that:

> [E]xposure of consumers' personal information has caused and is likely to cause substantial consumer injury, including financial injury, to consumers and businesses. For example, Defendants' failure to implement reasonable and appropriate security measures resulted in the three data breaches . . . the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and *more than $10.6 million in fraud loss. Consumers* and businesses suffered *financial injury*, including, but not limited to, *unreimbursed fraudulent charges*, increased costs, and lost access to funds or credit. Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm.

(Compl. ¶ 40 (emphasis added)). For purposes of resolving Hotels and Resorts' motion, these allegations must be "accepted as true." *See Iqbal*, 556 U.S. at 678.

Although the FTC alleges that both consumers *and* businesses suffered financial injury, Hotels and Resorts fails to cite any authority that necessarily preempts an unfairness action where the FTC alleges injury by both groups. Indeed, the FTC here alleges that at least some consumers suffered financial injury that included "unreimbursed financial injury" and, drawing inferences in favor of the FTC, the alleged injury to consumers is substantial. *See Am. Fin. Servs. Ass'n*, 767 F.2d at 972 ("An injury may be sufficiently substantial . . . if it does a small harm to a large number of people, or if it raises a significant risk of concrete harm.") (internal quotation marks and citations omitted).[13]

And the Court is not persuaded by Hotels and Resorts' argument that, since federal law places a $50 limit on the amount of consumer liability for any unauthorized use of a payment card, any alleged injury cannot be substantial. (HR's Mov. Br. at 19 (citing 15 U.S.C. § 1643(a)(1))). The FTC alleges *facts* to the contrary that the Court must accept as true, drawing

[13] Notably, Hotels and Resorts did not dispute the FTC's additional contention at oral argument that the FTC "can protect small businesses," (*see* 11/7/13 Tr. at 125:4-11), at oral argument or in supplemental briefing thereafter.

reasonable inferences in favor of the FTC, not Hotels and Resorts. *See Phillips v. Cnty. Of Allegheny*, 515 F.3d 224, 233-34 (3d Cir. 2008).[14]

Hotels and Resorts argues that the instant action is analogous to *Reilly*, where the Third Circuit affirmed dismissal of claims against a payroll-processing firm that was hacked because the plaintiffs had not suffered an "injury-in-fact." (HR's Mov. Br. at 20 (citing 664 F.3d at 40-41)). In *Reilly*, the Third Circuit set forth that

> Appellants have alleged no misuse, and therefore, no injury.
> . . . .
> In data breach cases where no misuse is alleged, however, there has been no injury—indeed, no change in the status quo. Here, Appellants' credit card statements are exactly the same today as they would have been had Ceridian's database never been hacked. Moreover, there is no quantifiable risk of damage in the future.
> . . . .
> Although Appellants have incurred expenses to monitor their accounts and to protect their personal and financial information from imminent misuse and/or identity theft . . . they have not done so as a result of any *actual* injury (e.g. because their private information was misused or their identities stolen). Rather, they prophylactically spent money to ease fears of future third-party criminality. Such misuse is only speculative—not imminent.

Reilly, 664 F.3d at 44, 45-46 (internal quotation marks and citations omitted).[15]

But here, as noted above, the FTC has alleged misuse. (*See, e.g.*, Compl. ¶ 40). Thus, the Court finds that *Reilly* does not compel a finding that the FTC's allegations regarding substantial injury are insufficient as a matter of law. *See* 664 F.3d at 45-46; *see also Anderson v.*

[14] The FTC and Hotels and Resorts dispute whether federal law provides liability protection for debit cards. (FTC's Opp. Br. at 8; HR's Reply Br. at 9). For the reasons discussed above, however, this issue is not material to the Court's resolution of Hotels and Resorts' motion to dismiss.

[15] The parties contest whether non-monetary injuries are cognizable under Section 5 of the FTC Act. (HR's Mov. Br. at 20 (citing *Reilly*, 664 F.3d at 46); FTC's Opp. Br. at 8-9 (citing *Neovi*, 604 F.3d at 1158; *Accusearch*, 570 F.3d at 1194); HR's Reply Br. at 9 (citing *Am. Fin. Servs. Ass'n*, 767 F.2d at 973 n.18; *Randolph v. ING Life Ins. & Annuity Co.*, 486 F. Supp. 2d 1, 8 (D.D.C. 2007))). Although the Court is not convinced that non-monetary harm is, as a matter of law, unsustainable under Section 5 of the FTC Act, the Court need not reach this issue given the analysis of the substantial harm element above.

Hannaford Bros. Co., 659 F.3d 151, 164-65 (1st Cir. 2011) (explaining that courts have reasoned that, "in the absence of unauthorized charges," plaintiffs "lacked a reasonable basis for fearing there would be unauthorized charges to their accounts as a result of the theft" and that this "*very reasoning suggests that these courts would reach a different result if the plaintiffs alleged that they had suffered fraudulent charges to their accounts*") (emphasis added).[16]

The FTC's allegations also permit the Court to reasonably infer that Hotels and Resorts' data-security practices *caused* theft of personal data, which ultimately *caused* substantial injury to consumers. The FTC alleges "a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft." (Compl. ¶ 24). And, making reasonable inferences in favor of the FTC, these practices correspond to the allegations involving how intruders perpetrated three data breaches, (*see id.* ¶¶ 25-39)—which ultimately resulted in the alleged substantial injury, (*id.* ¶ 40).

For instance, the FTC alleges that Defendants "failed to employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess" and "did not require the use of complex passwords for access to the Wyndham-branded hotels' property management systems and allowed the use of easily guessed passwords." (*Id.* ¶ 24(f)). Correspondingly, the FTC alleges that "intruders attempted to compromise an administrator account on the Hotels and Resorts' network by guessing multiple user IDs and passwords—known as a brute force attack." (*Id.* ¶ 26).

[16] Hotels and Resorts attempts to discredit *Anderson* because that case "arose solely under Maine law . . . so the court had no opportunity to address whether such minor injury-avoidance costs constitute unavoidable 'substantial injury' under the FTC Act." (HR's Reply Br. at 10). But much of the precedent cited by the parties involves analogous circumstances. In fact, Hotels and Resorts itself relies on a case involving analysis under state law. (HR's Mov. Br. at 22 ("[C]ourts examining data-security issues under state unfair-trade-practices statutes have held that such practices are unfair only when they are egregious or 'reckless' in nature." (citing *Worix v. MedAssets, Inc.*, 869 F. Supp. 2d 893, 900 (N.D. Ill. 2012))).

Similarly, the FTC alleges that Defendants "failed to adequately inventory computers connected to Hotels and Resorts' network so that Defendants could appropriately manage the devices on its network." (*Id.* ¶ 24(g)). And the FTC correspondingly alleges that, since "Defendants did not have an adequate inventory of the Wyndham-branded hotels' computers connected to its network . . . they were unable to physically locate those computers" and, therefore, "Defendants did not determine that Hotels and Resorts' network had been compromised until almost four months later." (*Id.* ¶ 27).

Likewise, the FTC alleges that Defendants failed to "use readily available security measures to limit access between and among the Wyndham-branded hotels' property management systems," such as firewalls. (*Id.* ¶ 24(a)). And this aligns with the FTC's allegation that intruders "were able to gain unfettered access to the property management systems servers of a number of hotels" because "Defendants did not appropriately limit access between and among the Wyndham-branded hotels' property management systems, Hotels and Resorts' own corporate network, and the Internet—such as through the use of firewalls." (*Id.* ¶ 28).

Finally, the FTC alleges that this "failure to implement reasonable and appropriate security measures exposed consumers' personal information to unauthorized access, collection, and use" and "has caused and is likely to cause substantial consumer injury, including financial injury, to consumers and businesses." (*Id.* ¶ 40). Drawing inferences in favor of the FTC, the identified failures caused the breaches, resulting in the alleged substantial injury. *See Phillips*, 515 F.3d at 231.

At its root, Hotels and Resorts' challenge to the FTC's injury and causation allegations is essentially an appeal for a heightened pleading standard. Hotels and Resorts seems to ask this

Court to read a "recklessness or egregiousness" requirement into the statutorily-defined unfairness standard. (*See* HR's Mov Br. at 22). Similarly, it argues that the FTC should have to plead the precise consumer harm, the "exact alleged deficiencies" that caused the "theft of the information," and how the breaches caused the alleged harm—because, as a government agency, the FTC conducted a pre-suit investigation. (*Id.* at 23; 11/7/13 Tr. at 101:13-102:14, 104:19-23, 108:3-7).

But the Court declines to impose such a heightened standard because Hotels and Resorts cites no authority to this effect. (*See*, *e.g.*, HR's Mov. Br. at 23 (stating that, "[a]fter a two-year investigation into [Hotels and Resorts'] data-security practices, surely the FTC should be required to say more about how the alleged vulnerabilities 'result[ed]' in consumer harm," but citing no authority)).

ii. *"Reasonably avoidable" allegations*

Second, the FTC adequately pleads that the alleged substantial injury *was not reasonably avoidable*. Hotels and Resorts argues that "[c]onsumers can . . . always 'reasonably avoid' any financial injury stemming from the theft of payment card data simply by having their issuer rescind any unauthorized charges." (HR's Mov. Br. at 19 (citing 15 U.S.C. § 1643(a)(1)); *see also* HR's Reply Br. at 9 ("Even accepting as true the FTC's unsubstantiated allegation that some consumers might not have been reimbursed . . . federal law and card-brand zero-liability policies make clear that any such charges were nonetheless 'reasonably avoidable' by consumers.")). Hotels and Resorts thus effectively asks the Court to hold that, as a matter of law, any financial injury from payment card theft data is reasonably avoidable and that the FTC's allegation to the contrary, (Compl. ¶¶ 40, 43, 48), could not be true under any factual scenario.

But the Court cannot make such a far-reaching conclusion regarding an issue that seems fact-dependent. *See FTC v. Inc21.com*, 745 F. Supp. 2d 975, 1004 (N.D. Cal. 2010) (granting summary judgment in favor of the FTC and finding that the "unrebutted evidence supports a finding that the harm suffered by consumers was not reasonably avoidable").

iii. *Other purportedly "conclusory" allegations*

Third, the Court is not persuaded that the FTC's complaint otherwise fails federal pleading standards. Hotels and Resorts criticizes the FTC's use of terms such as "readily available," "adequate," "commonly-used," and "proper." (HR's Mov. Br. at 22 (quoting Compl. ¶ 24)). Hotels and Resorts argues that the "FTC does not give any factual detail as to what procedures, or combination of procedures, would have met those conclusory standards" and that the FTC "does not explain what measures would be 'reasonable.'" (*Id.*).

But the FTC does not merely allege that Hotels and Resorts' practices were unreasonable. *Cf. Willey v. J.P. Morgan Chase, N.A.*, No. 09-1397, 2009 WL 1938987, at *4 (S.D.N.Y. July 7, 2009) (finding that plaintiff did "not support [his] formulaic recitations with factual allegations that describe any insufficiency in [defendant's] security procedures, or with allegations that [defendant] lacked such procedures" or "how the procedures [defendant] adopted failed to comply with the [relevant] [g]uidelines").

Instead, the FTC describes several data-security insufficiencies, including: failing to employ firewalls; permitting "storage of payment card information in clear readable text"; failing to make sure Wyndham-branded hotels "implemented adequate information security policies and procedures prior to connecting their local computer networks to Hotels and Resorts' computer network"; permitting Wyndham-branded hotels "to connect insecure servers to Hotels and Resorts' networks, including servers using outdated operating systems that could not receive

security updates or patches to address known security vulnerabilities"; permitting servers on Hotels and Resorts' networks with commonly-known default user IDs and passwords; failing to "employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess"; failing to "adequately inventory computers connected to Hotels and Resorts' network" to manage devices on its network; failing to "monitor Hotels and Resorts' computer network for malware used in a previous intrusion"; and failing to restrict third-party access "such as by restricting connections to specified IP addresses or granting temporary, limited access, as necessary." (Compl. ¶¶ 24(a)-(j)).

The FTC therefore does more than simply assert "that a violation . . . must have occurred simply because the data loss incident occurred." *Cf. Willey*, 2009 WL 1938987, at *4. It alleges insufficiencies that, drawing reasonable inferences in favor of the FTC, led to data-security breaches. (*See* Compl. ¶¶ 24-39).

And, although the FTC does not plead the particularized data-security rules or regulations that Hotels and Resorts' procedures allegedly failed to comply with, this cannot preclude the FTC's enforcement action. *See Sperry & Hutchinson Co.*, 405 U.S. at 239-40; *Colgate-Palmolive Co.*, 380 U.S. at 384-85; *PBW Stock Exch.*, 485 F.2d at 732 (citing *Chenery Corp.*, 332 U.S. at 203). Indeed, Hotels and Resorts' challenge to this effect seems to be a repackaging of its fair notice argument—which this Court has considered and rejected.

B. The FTC's Deception Claim (Count One)

Hotels and Resorts also challenges the FTC's deception claim. (HR's Mov. Br. at 23). In this claim, the FTC cites the Defendants' privacy policy disseminated on Hotels and Resorts' website and alleges that, "in connection with the advertising, marketing, promotion, offering for sale, or sale of hotel services, Defendants have represented, directly or indirectly, expressly or by

implication, that they had implemented reasonable and appropriate measures to protect personal information against unauthorized access"—but that "Defendants did not implement reasonable and appropriate measures to protect personal information against unauthorized access." (Compl. ¶¶ 21, 44-45). Accordingly, the FTC alleges that Defendants' representations "are false or misleading and constitute deceptive acts or practices" under Section 5(a) of the FTC Act. (*Id.* ¶ 46).

1. The parties' contentions

Hotels and Resorts argues that the FTC's deception claim is insufficiently pleaded under either a heightened pleading requirement pursuant to Federal Rule of Civil Procedure 9(b) or the general pleading standard. (HR's Mov. Br. at 23-24). Hotels and Resorts contends that—although its online privacy policy was allegedly deceptive—the FTC "relies primarily on allegations concerning the state of data-security *at the Wyndham-branded hotels*." (*Id.* at 24).

To that extent, Hotels and Resorts asserts that the Wyndham-branded hotels are "legally separate entities that each maintain their own computer networks and engage in their own data-collection practices." (*Id.* at 24-25). Indeed, Hotels and Resorts avers that its privacy policy specifically *excludes* the Wyndham-branded hotels from the policy's data-security representations and that such exclusion of responsibility over franchisees' actions is consistent with franchise law. (*Id.* at 25-27).

Further, Hotels and Resorts argues that the FTC's allegations concerning Hotels and Resorts' own data-security practices "amount to nothing more than conclusory statements of wrongdoing that fall well short of establishing a 'plausible' claim to relief." (*Id.* at 27 (citing *Iqbal*, 556 U.S. at 678)). Hotels and Resorts argues that the FTC fails to allege what data-

security practices were "standard" in the hospitality industry or how Hotels and Resorts' practices fell short. (*Id.*).

Finally, Hotels and Resorts asserts that the FTC "does nothing to explain how the alleged deficiencies it identifies placed personal information *collected by [Hotels and Resorts]* at risk" and, therefore, there is "no basis in law or logic for pointing to the data breaches as evidence of 'deceptive' practices by [Hotels and Resorts]." (*Id.* at 28).

In opposition, the FTC asserts that, although a Section 5 claim of deceptive practices need not meet the Rule 9(b) heightened pleading standard, its complaint does so. (FTC's Opp. Br. at 26-27). The FTC argues that Hotels and Resorts, in fact, concedes certain allegations "are relevant to the data security measures of the Wyndham entities" and, therefore, that it has sufficiently pleaded a claim for deceptive data-security practices. (*Id.* at 28 (citing Compl. ¶¶ 24(g)-(i))).

The FTC also argues that it alleges that Hotels and Resorts was responsible for data-security failures by "permit[ing] computers with unreasonable data security measures on its network." (*Id.* at 27 (citing Compl. ¶ 24)). The FTC avers that, since the alleged data-security failures are "attributable" to Hotels and Resorts, the FTC need not plead "actual control" over the Wyndham-branded hotels' activities. (*Id.* at 28). The FTC adds, however, that the complaint nevertheless pleads such control "over the relevant aspects of the franchisees' data security practices." (*Id.* (citing Compl. ¶¶ 15, 17-19)).

2. <u>Analysis</u>

As an initial matter, the parties dispute whether the FTC must meet a heightened pleading standard under Federal Rule of Civil Rule 9(b) when alleging unlawful deception. District courts

have reached different conclusions as to whether claims under the FTC Act must satisfy Rule 9(b)'s heightened pleading standard.[17] This is an issue of first impression in this District.

Rule 9(b) provides that, "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." To establish liability for the deception prong of Section 5(a), "the FTC must establish: '(1) there was a representation; (2) the representation was likely to mislead customers acting reasonably under the circumstances, and (3) the representation was material.'" *FTC v. Millennium Telecard, Inc.*, No. 11-2479, 2011 WL 2745963, at *3 (D.N.J. July 12, 2011) (quoting *FTC v. Tashman*, 318 F.3d 1273, 1277 (11th Cir. 2003)).[18]

This Court is not convinced that the FTC's deception claim requires Rule 9(b) treatment. *See FTC v. Freecom Commc'ns, Inc.*, 401 F.3d 1192, 1203 n.7 (10th Cir. 2005) ("A § 5 claim simply is not a claim of fraud as that term is commonly understood or as contemplated by Rule 9(b), and the district[] court's inclination to treat it as such unduly hindered the FTC's ability to present its case."). Indeed, Hotels and Resorts summarily asserts that the FTC's claim "'sounds in fraud,'" without any reasoning or analysis. (*See* HR's Mov. Br. at 24 (quoting *Lights of Am.*, 760 F. Supp. 2d at 853; *Ivy Capital*, 2011 WL 2118626, at *3)); *see also Med. Billers Network*,

[17] Some courts have explicitly ruled that Rule 9(b)'s heightened pleading standard does not apply. *See, e.g., FTC v. Sterling Precious Metals, LLC*, No. 12-80597, 2013 WL 595713, at *3 (S.D. Fla. Feb. 15, 2013); *FTC v. Consumer Health Benefits Ass'n*, No. 10-3551, 2012 WL 1890242, at *6-7 (E.D.N.Y. May 23, 2012); *FTC v. Innovative Mktg., Inc.*, 654 F. Supp. 2d 378, 388 (D. Md. 2009); *FTC v. Med. Billers Network*, 543 F. Supp. 2d 283, 314-15 (S.D.N.Y. 2008). Others have found that it does apply. *See, e.g., FTC v. Ivy Capital, Inc.*, No. 11-283, 2011 WL 2118626, at *3 (D. Nev. May 25, 2011); *FTC v. Lights of Am., Inc.*, 760 F. Supp. 2d 848, 852-54 (C.D. Cal. 2010).

[18] Hotels and Resorts does not dispute the materiality element of this standard. *See also In re Nat'l Credit Mgmt. Grp., L.L.C.*, 21 F. Supp. 2d 424, 441 (D.N.J. 1998) ("Explicit claims or deliberately-made implicit claims utilized to induce the purchase of a service or product are presumed to be material.").

543 F. Supp. 2d at 314 (explaining that Defendants do not "explain why the pleading requirements of Rule 9(b) should apply to this action").[19]

Nevertheless, the Court finds that, even under a Rule 9(b) heightened standard, the allegations here suffice. *See FTC v. Cantkier*, 767 F. Supp. 2d 147, 154-55 (D.D.C. 2011) ("[A] claim for deceptive acts or practices under Section 5 is not a fraud claim. . . . [T]he Court does not need to rule on the applicability of Rule 9(b) to Section 5 actions here because, even assuming *arguendo* that Rule 9(b) applies, the FTC's allegations have been pled with sufficient particularity.").

Here, the FTC alleges that Defendants "disseminated[] or caused to be disseminated" privacy policies or statements, including statements "regarding the privacy and confidentiality of personal information [] disseminated on the Hotels and Resorts' website." (Compl. ¶ 21 (reproducing a portion of the privacy policy statement disseminated on the Hotels and Resorts' website)). The statement from Hotels and Resorts' website represents, in part, that "[w]e safeguard our Customers' personally identifiable information by using industry standard practices" and make "commercially reasonable efforts" to collect personally identifiable information "consistent with all applicable laws and regulations" and, among other things, that "[w]e take commercially reasonable efforts to create and maintain 'fire walls' and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent with this Policy." (*Id.*).

The FTC also alleges that Defendants "failed to adequately inventory computers connected to the Hotels and Resorts' network so that Defendants could appropriately manage the

[19] At most, Hotels and Resorts' contention seems to be premised on a nefarious, intent-like element that is purportedly inherent in a deception claim. (*See* 11/7/13 Tr. at 137:20-138:6, 146:22-147:3). But, "[u]nlike the elements of common law fraud, the FTC need not prove scienter, reliance, or injury to establish a § 5 violation." *Freecom Commc'ns*, 401 F.3d at 1203 n.7.

devices on its network," "failed to employ reasonable measures to detect and prevent unauthorized access to Defendants' computer network or to conduct security investigations," and "failed to follow proper incident response procedures, including failing to monitor Hotels and Resorts' computer network for malware used in a previous intrusion." (*Id.* ¶¶ 24(g)-(i) (identifying various practices that allegedly exposed consumers' personal data)).

Hotels and Resorts dismisses these allegations as "conclusory statements of wrongdoing." (HR's Mov. Br. at 27 (asserting that "the FTC makes a half-hearted attempt to allege that [Hotels and Resorts] made deceptive statements about *its own* data-security practices")). But the Court is not so persuaded. Indeed, Hotels and Resorts' argument again seems to be a repackaging of its fair-notice challenge. (*See* 11/7/13 Tr. at 141:9-16). The Court has, however, already rejected this challenge.

Moreover, accepting Hotels and Resorts' position leads to the following incongruous result: Hotels and Resorts can explicitly represent to the public that it "safeguard[s] . . . personally identifiable information by using industry standard practices" and makes "commercially reasonable efforts" to make collection of data "consistent with all applicable laws and regulations"—but that, as a matter of law, the FTC cannot even file a complaint in federal court challenging such representations without first issuing regulations. *See Voegele*, 625 F.2d at 1078-79; *see also Iqbal*, 556 U.S. at 679 ("Determining whether a complaint states a plausible claim for relief will . . . be a context-specific task that requires the reviewing court to draw on its judicial experience and common sense.").

Furthermore, the Court is not convinced that the FTC's other allegations mandate dismissal of its deception claim because, according to Hotels and Resorts, they "concern[] the state of data-security *at the Wyndham-branded hotels*" and that the three breaches involved

cybercriminals accessing "payment-card data collected and controlled by the Wyndham-branded hotels." (HR's Mov. Br. at 24). The Court is not so convinced for the following two reasons.

First, the Court cannot accept Hotels and Resorts' contention, that, *as a matter of law*, it is necessarily a separate entity from Wyndham-branded hotels such "that each maintain their own computer networks and engage in their own data-collection practices." (*Id.* at 24-25). After all, the FTC alleges that "Defendants failed to provide reasonable and appropriate security for the personal information collected and maintained by Hotels and Resorts, Hotel Management, and the Wyndham-branded hotels, by engaging in a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft," including Defendants' failure "to ensure the Wyndham-branded hotels implemented adequate information security policies and procedures prior to connecting their local networks to Hotels and Resorts' computer network." (Compl. ¶¶ 24, 24(c)). And, accepting the FTC's factual allegations as true and drawing reasonable inferences in favor of the FTC, the Court finds that these allegations support the FTC's deception claim against Hotels and Resorts.[20]

Second, the Court is not persuaded by Hotels and Resorts' arguments involving disclaimer. (*See* HR's Mov. Br. at 25). Hotels and Resorts contends that the policy defines "we," "us," and "our" in a certain way that excludes Wyndham-branded hotels, applies to "our

[20] Alternatively, the Court finds that the FTC's complaint sufficiently pleads Hotels and Resorts' control over the Wyndham-branded hotels. (*See* Compl. ¶¶ 15, 17-19); *Cf. Chen v. Domino's Pizza, Inc.*, No. 09-107, 2009 WL 3379946, at *4 (D.N.J. Oct. 16, 2009) ("Plaintiffs' complaint does not contain a single factual allegation indicating that Domino's had any authority or control over their employment conditions.").

Tellingly, Hotels and Resorts' responds that "the allegations in the complaint do not establish that [Hotels and Resorts] exercised the kind of 'day-to-day' control that is necessary to assign vicarious liability to a franchisor"—but cites a case resolved at summary judgment. (HR's Reply Br. at 11 (citing *Capriglione v. Radisson Hotels Int'l, Inc.*, No. 10-2845, 2011 WL 4736310, at *3 (D.N.J. Oct. 5, 2011))); *see also Drexel v. Union Prescription Ctrs., Inc.*, 582 F.2d 781, 786, 789-90 (3d Cir. 1978) (finding that, "on the present record genuine issues of material fact exist regarding the nature of the relationship between appellee and its franchisee which preclude the entry of summary judgment" and explaining that "[w]hether the control retained by the franchisor is also sufficient to establish a master-servant relationship depends in each case upon the nature and extent of such control as defined in the franchise agreement or by the actual practice of the parties").

collection" of data, and only applies "to the extent we control the Information." (*Id.* at 25 (quoting D.E. No. 91-3, Ex. A to Declaration of Jennifer A. Hradil ("Hradil Decl.") at 1)). Hotels and Resorts also cites language in the policy that purportedly "*expressly disclaims* making any representations about the security of payment-card data collected by the Wyndham-branded hotels." (*Id.* at 25 (citing Ex. A to Hradil Decl. at 4)).

Hotels and Resorts thus asserts that "any reasonable consumer, after reading the privacy policy 'as a whole, without emphasizing isolated words or phrases apart from their context' . . . would have understood that the policy made statements only about data-security practices at [Hotels and Resorts] and made no representations about data-security practices at the Wyndham-branded hotels." (*Id.* at 25-26 (citation omitted) (quoting *Millennium Telecard*, 2011 WL 2745963, at *5)).

But the policy also recognizes "the importance of protecting the privacy of individual-specific (personally identifiable) information collected about guests" and states that it "applies to residents of the United States, *hotels of our Brands located in the United States*, and Loyalty Program activities in the United States only." (Ex. A to Hradil Decl. at 1 (emphasis added)). And it also states that "[w]e take commercially reasonable efforts to create and maintain 'fire walls' and other appropriate safeguards to ensure that to the extent we *control* the Information, the Information is used only as authorized by us and consistent with this Policy." (Ex. A at 1 (emphasis added)).

Thus, it is reasonable to infer the exact opposite of what Hotels and Resorts posits: that a reasonable customer would have understood that the policy makes statements about data-security practices at Hotels and Resorts *and* Wyndham-branded hotels, to the extent that Hotels and Resorts *controls* personally identifiable information. And, for this reason, the Court finds

unpersuasive Hotels and Resorts' argument that the FTC "does nothing to explain how the alleged deficiencies it identifies placed personal information *collected by [Hotels and Resorts]* at risk." (*See* HR's Mov. Br. at 28).

The Court is not persuaded otherwise by Hotels and Resorts' reliance on case law purportedly involving "similar disclaimers to dismiss deception or fraud-based claims." (HR's Reply Br. at 11 (citing *Pathfinder Mgmt., Inc. v. Mayne Pharma PTY*, No. 06-2204, 2008 WL 3192563, at *16 (D.N.J. Aug. 5, 2008); *Eckler v. Wal-Mart Stores, Inc.*, No. 12-727, 2012 WL 5382218, at *7 (S.D. Cal. Nov. 1, 2012))). As such, *Pathfinder Management* involved a disclaimer that "explicitly states that [p]laintiff is aware that no representations are being made to them outside those contained within the Purchase Agreement and specified schedules and instruments." 2008 WL 3192563, at *16. Notwithstanding this disclaimer, the plaintiff sought to bring certain allegations "based upon representations made outside of the Purchase Agreement," which the Court determined could not "be the basis for alleging fraudulent misrepresentation or fraud in the inducement." *Id.*

Here, however, the allegations regarding the privacy policy do not relate to extrinsic evidence, and Hotels and Resorts does not explain how the FTC's allegations are otherwise analogous to those in *Pathfinder Management.* For similar reasons, the Court is not persuaded by *Eckler*. *See* 2012 WL 5382218, at *7 (dismissing claims where extrinsic evidence in the form of studies allegedly supported plaintiff's claims that a dietary supplement's representations were false or misleading).

Again, at this stage, the Court must draw reasonable inferences in favor of the FTC, not Hotels and Resorts—even if the FTC's deception claim warrants Rule 9(b) treatment. *See Flood v. Makowski*, No. 03-1803, 2004 WL 1908221, at *14 (M.D. Pa. Aug. 24, 2004) ("While Rule

9(b) requires pleading with specificity, it does not erase the general standard that the Court should draw reasonable inferences in favor of Plaintiffs." (citing *Lum v. Bank of Am.*, 361 F.3d 217 (3d Cir. 2004))).

Moreover, the impression that a reasonable consumer would have had after reading the privacy policy seems to involve fact issues that the Court cannot resolve at this juncture. *See FTC v. Nat'l Urological Grp., Inc.*, 645 F. Supp. 2d 1167, 1189 (N.D. Ga. 2008) ("The meaning of an advertisement, the claims or net impressions communicated to reasonable consumers, is fundamentally a question of fact."); *see also Am. Home Prods. Corp. v. FTC*, 695 F.2d 681, 687 (3d Cir. 1982) ("The impression created by the advertising, not its literal truth or falsity, is the desideratum.").

For these reasons, the Court cannot dismiss the FTC's deception claim at this juncture.

V. CONCLUSION

As set forth above, the Court hereby DENIES Hotels and Resorts' motion to dismiss. An appropriate Order accompanies this Opinion.

/s/ Esther Salas
Esther Salas, U.S.D.J.