UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Edith Ramirez, Chairwoman
Maureen K. Ohlhausen
Terrell McSweeney

In the Matter of
Docket No. 9357
PUBLIC

LABMD, INC.,
a corporation.

ORDER CORRECTING ORAL ARGUMENT TRANSCRIPT

On May 4, 2016, Complaint Counsel filed an unopposed Motion to correct the transcript of the Oral Argument held in this proceeding on March 8, 2016. The Motion states that Complaint Counsel conferred with counsel for Respondent in a good faith effort to stipulate to the desired corrections, as prescribed by Commission Rule 3.52(i), 16 C.F.R. § 3.52(i), and that while Respondent has declined to join the Motion, Respondent agrees to the proposed corrections and will not oppose the Motion. Accordingly,

IT IS ORDERED THAT the Oral Argument Transcript be, and it hereby is, modified to adopt the two corrections requested by Complaint Counsel in the May 4 Motion, and to read as shown in the attached corrected copy.

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: May 16, 2016
UNITED STATES OF AMERICA

BEFORE THE FEDERAL TRADE COMMISSION

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

In the Matter of

) Docket No. 9357
)
LabMD, Inc.,

a corporation.

March 8, 2016
1:00 p.m.

ORAL ARGUMENT

Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C.

Reported by: Josett F. Whalen, Court Reporter
APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:

LAURA RIPOSO VANDRUFF, ESQ.
Federal Trade Commission
Bureau of Consumer Protection
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
(202) 326-2999
lvandruff@ftc.gov

ON BEHALF OF LABMD, INC.:

ALFRED J. LECHNER, JR., ESQ.
Cause of Action
1919 Pennsylvania Avenue, N.W.
Suite 650
Washington, D.C. 20006
(202) 499-4231
JLechner@CauseOfAction.org
CHAIRWOMAN RAMIREZ: Good afternoon, everyone.

The Commission is meeting today in open session to hear oral argument in the matter of LabMD, Docket Number 9357, on the appeal of counsel supporting the complaint from the initial decision issued by the Administrative Law Judge.

Complaint counsel are represented by Ms. Laura VanDruff, and the respondent is represented by Mr. Alfred J. Lechner, Jr.

During this proceeding, each side will have 45 minutes to present their arguments. Complaint counsel shall make the first presentation and will be permitted to reserve time for rebuttal, and then counsel for respondent will then make his presentation. Complaint counsel may conclude the argument with their rebuttal.

Ms. VanDruff, do you wish to reserve any time for rebuttal?

MS. VANDRUFF: I do. Thank you, Madam Chairwoman. Ten minutes, please.

CHAIRWOMAN RAMIREZ: You may begin.

MS. VANDRUFF: Thank you, Madam Chairwoman.

Madam Chairwoman, and may it please the
This is a case about a company whose very business model depended on collecting and maintaining hundreds of thousands of consumers' most sensitive categories of personal information, including names, dates of birth, Social Security numbers, health insurance information and medical diagnoses, but LabMD did not put in place even the most basic protections to secure that information from unauthorized disclosure.

LabMD's multiple, systemic and serious failures violated section 5 of the FTC Act because they unlawfully caused or likely caused substantial consumer injury that consumers could not avoid and that was not outweighed by countervailing benefits to consumers or competition.

Applying the settled law of the Commission, this is not a close case for the Commission in its de novo review of the record on appeal. But before I review the overwhelming evidence in this case, it's important to first address the initial decision's three most significant errors of law that complaint counsel is challenging.

First, the initial decision was wrong in holding that an act or practice that raises a significant risk of concrete harm does not cause
substantial consumer injury.

This Commission has recognized that a practice causes or likely causes substantial -- excuse me -- that -- this Commission has recognized that a practice causes or is likely to cause substantial injury if it raises a significant risk of concrete harm.

The Commission's holding is grounded in Section 5(n), which codified the unfairness statement. And the Commission's reasoning is affirmed by case law applying primary sources. The standard is consistent with the Commission's broad mandate to prevent acts or practices that injure the public.

The initial decision's ruling to the contrary cannot be reconciled with this authority, which is controlling in this case and in any data security case brought under the FTC's unfairness authority.

Second --

COMMISSIONER OHLHAUSEN: Counsel, could I just ask you a question on that first prong, the first “error,” that you're arguing?

MS. VANDRUFF: Yes.

COMMISSIONER OHLHAUSEN: Are you saying that raising a significant risk of concrete harm equals substantial injury, or that it is likely to cause substantial injury?
MS. VANDRUFF: Nothing about the law of Section 5 has changed since the Commission issued its opinion on the motion to dismiss in January of 2014. And in that opinion, the Commission held that an 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.

And to back up for a moment, Commissioner Ohlhausen, the Commission's order on that motion to dismiss also observed that actual, completed economic harms are not necessary to substantiate that a firm's data security activities caused or likely caused consumer injury and thus constitute unfair acts or practices.

Therefore, for data security practices to be unfair without the occurrence of a breach, it must follow that for -- that what makes poor data security practices actionable under Section 5 is the risk of concrete harm that they --

CHAIRWOMAN RAMIREZ: Counsel, I want to spend a little bit of time here on the legal standard.

MS. VANDRUFF: Yes.

CHAIRWOMAN RAMIREZ: Can you tell me -- so your position is that there was actual harm in this case; correct?
MS. VANDRUFF: That's correct.

CHAIRWOMAN RAMIREZ: And could you outline for me what that actual harm was.

MS. VANDRUFF: So to go back to Commissioner Ohlhausen's question, the actual harm was the significant risk of concrete harm that was created by the data security practices and the failures of adequate security that LabMD undertook in not safeguarding adequately the sensitive personal information for 750,000 consumers.

CHAIRWOMAN RAMIREZ: Counsel, I'd like you to answer the question -- what does the likely -- likelihood piece of the unfairness standard mean? Respondent is arguing that, if one were to accept your position, you're effectively reading out of the statute the word "likely," so can you explain to me then, what is the meaning of that second part of the unfairness test?

MS. VANDRUFF: It doesn't -- it doesn't render "likely" moot at all. A likely substantial injury remains cognizable also. There's no change to that standard at all.

CHAIRWOMAN RAMIREZ: So again, I'm just trying to understand what "likely to cause" means, and is that distinct
from actual harm? Because you're arguing that risk -- a significant risk of concrete harm -- constitutes actual harm, correct?

MS. VANDRUFF: Yes.

CHAIRWOMAN RAMIREZ: So how distinct is the "likely to cause substantial harm" prong of the unfairness test? Does that mean anything different?

MS. VANDRUFF: I want to make sure that I understand your question.

A significant risk of concrete harm is itself substantial injury. If that injury is -- occurs -- if that injury is occurring at present, if the acts or practices of a company cause that injury to occur, then that risk occurs at present.

CHAIRWOMAN RAMIREZ: So let me frame it a little bit differently. If your position is that a significant risk of concrete harm is a completed harm, tell me how you would go about establishing a likelihood of substantial injury. I'm trying to see if there's a distinction there.

MS. VANDRUFF: Right.

Well, I -- I want to --

CHAIRWOMAN RAMIREZ: It's a different standard, right, it means something different. Does "actual harm"
mean something different than "likely to cause substantial injury"? There's a different standard of proof presumably under that piece of the --

MS. VANDRUFF: The likely, yes.

CHAIRWOMAN RAMIREZ: Yes.

MS. VANDRUFF: So to show that something would be "likely" would suggest that it would occur in the future, and so -- so that is --

CHAIRWOMAN RAMIREZ: So a temporal distinction.

MS. VANDRUFF: It's a temporal distinction, as we set forth in our briefing, that is correct.

Madam Chairwoman, yes.

If there are no further questions on that subject, then what I would move on to is the second error in the initial decision, and that is that the initial decision was wrong in holding that Section 5 requires proof of known identity theft.

Indeed, this Commission in this proceeding has held that the FTC permits the Commission to challenge multiple and systemic data security failures even where no breach has occurred.

And finally, the initial decision was wrong --

COMMISSIONER OHLHAUSEN: Counselor, can I ask, is that --

MS. VANDRUFF: Yes.
COMMISSIONER OHLHAUSEN: -- because systemic failures are likely to cause substantial injury or that they themselves cause substantial injury?

That is, complaint counsel doesn't have to show that there's a breach because the failures are likely to cause substantial injury?

MS. VANDRUFF: Commissioner Ohlhausen, I believe that the reasoning for the Commission's observation that complaint counsel need not show proof of a breach is because a significant risk of concrete harm is sufficient to show substantial injury, as I set forth in response to your initial question.

And finally, the initial decision was wrong in requiring complaint counsel to present expert testimony quantifying the probability of injury.

Section 5 does not impose this requirement.

Rather, complaint counsel must present and did present reasonably available evidence of the risk posed to consumers by a company's poor data security practices.

LabMD's data security practices exemplify the conduct against which the FTC Act protects consumers. Its practices caused or were likely to cause significant risk of the concrete harms of identity theft, medical
identity theft, and the unauthorized disclosure for hundreds of thousands of consumers, most of whom had probably never heard of LabMD.

CHAIRWOMAN RAMIREZ: Was there any other actual harm other than the significant risk that you've already cited?

MS. VANDRUFF: So at the outset, that's correct, Madam Chairwoman, that there was a significant risk created for 750,000 consumers.

CHAIRWOMAN RAMIREZ: Okay. So putting that aside, was there any other --

MS. VANDRUFF: So putting that aside --

CHAIRWOMAN RAMIREZ: -- completed harm that the evidence demonstrates, in your view?

MS. VANDRUFF: Right.

Putting aside the 750,000 consumers, that the record shows that there was also a file of 9300 consumers that was exposed on the peer-to-peer network.

CHAIRWOMAN RAMIREZ: So the exposure of the 1718 File itself is also actual, completed harm; is that --

MS. VANDRUFF: That's correct.

CHAIRWOMAN RAMIREZ: And anything else?

MS. VANDRUFF: And in addition, there was a file
containing the sensitive personal information of
approximately 600 consumers found in the hands of
identity thieves in Sacramento, California.

COMMISSIONER McSWEENY: Can I ask you a question
about the Sacramento file?

Do you agree with the ALJ's finding that there
is no evidence establishing that the Sacramento
documents were obtained from LabMD's computer network?

MS. VANDRUFF: So we are not conceding that the
Sacramento day sheets -- well, the evidence in the
record does not establish how the documents got from
LabMD to the identity thieves in Sacramento, but we
have established that they are LabMD documents containing
sensitive consumer information, and the fact that they
were obtained by identity thieves demonstrates exactly
the types of concrete injury that result from the
unauthorized disclosure of consumers' sensitive personal
information.

COMMISSIONER McSWEENY: I understood that
Dr. Hill's testimony basically asserted that he found that
the physical security at LabMD was reasonable, or was not
unreasonable.

So is that relevant here for establishing where
these documents came from?

MS. VANDRUFF: Well, as an initial matter, I
would disagree with that characterization of Professor Hill's opinion.

While the allegations of the complaint -- well, first of all, Professor Hill's opinions do not relate to physical security. And the allegations of the complaint also relate primarily to failures of electronic security, and those are the focus of Professor Hill's opinions. But the principles of the complaint and the principles of her opinions are equally applicable to physical security.

So, for example, LabMD's failure to have a written security --

CHAIRWOMAN RAMIREZ: Complaint Counsel, does your complaint -- the allegations in the complaint, do they relate to computer security or physical security?

The ALJ seemed to understand the complaint to be and the allegations in the case to be solely limited to computer security. Is that inaccurate?

MS. VANDRUFF: The allegations of the complaint relate to electronic security, but the principles are equally applicable to physical security.

So, for example, Madam Chairwoman, the allegations include a failure to have a written security policy, and LabMD's failure to have a written security
plan or to perform risk assessments created an environment in which significant risks to physical security were possible.

CHAIRWOMAN RAMIREZ: So I want to make very clear, notwithstanding the fact that the complaint in paragraph 10 focuses on computer security, are you saying the charges here and the evidence showed that there were also lapses in physical security? Is that what you're saying?

MS. VANDRUFF: I'm saying there's nothing inconsistent about our proofs to not -- to foreclose conclusions about physical security.

CHAIRWOMAN RAMIREZ: Okay. So you're also including physical security, that's part of the language that's used in the complaint, you're including lapses of physical security in the charges.

MS. VANDRUFF: That's right. The "Among other things" paragraph, Madam Chairwoman, is not an exhaustive list, and so certainly those are examples of the kinds of failures, and as examples, they extend to the kinds of things, including physical security, that's correct.

CHAIRWOMAN RAMIREZ: Okay.

MS. VANDRUFF: So LabMD's data security
practices exemplify the kinds of conduct against which
the FTC Act protects consumers, and its practices caused
or were likely to cause a significant risk of the kinds
of concrete harms like identity theft, medical identity
theft, and the unauthorized disclosure of sensitive
personal information.

And when a company's corporate network contains
hundreds of thousands of consumers' sensitive personal
information, Section 5 of the FTC Act requires a company
to take steps to protect it.

CHAIRWOMAN RAMIREZ: Counsel, so going back to
just focusing on the Sacramento documents --

MS. VANDRUFF: Yes.

CHAIRWOMAN RAMIREZ: -- as

the plaintiff in this matter, what obligation do you
have to establish a causal link between that exposure of
documents and the security practices of respondent, so
what amount of proof do you need to establish that
there's a link between that and the documents, and how
have you shown that?

MS. VANDRUFF: Right.

So we -- the record evidence, we have presented
evidence from the detectives in Sacramento that
demonstrate that the documents that came from LabMD
were found in the hands of identity thieves.
And while we have not been able to establish how those documents came to -- from LabMD to be in the hands of identity thieves, we have demonstrated that the kinds of information that LabMD maintains are the kinds of information that identity thieves value, and so it is very much a concrete harm that consumers will suffer if information that LabMD maintains is exposed without authorization.

COMMISSIONER OHLHAUSEN: I have a question that relates to that.

In your appeal brief on page 7, you said that LabMD created a significant risk of harm by collecting, storing and transferring consumer data in large volumes on a daily basis.

Under your theory, is that a significant risk equal to a substantial injury, or does there need to be something more? Just the fact that they collected sensitive health information, is that enough or does there need to be more, if we're just looking at a significant risk?

MS. VANDRUFF: The collection alone does not create a significant risk. It's the failure to adequately protect that data, the failure to safeguard that data from unauthorized disclosure, and that is the record that we have established in this case.
COMMISSIONER OHLHAUSEN: So that goes to whether they took reasonable precautions; is that right?

MS. VANDRUFF: That's correct.

COMMISSIONER OHLHAUSEN: Reasonable precautions? And so in the Wyndham case, they talk about a cost-benefit analysis that considers a number of relevant factors, such as the -- I'm quoting here -- "the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from an investment in stronger cybersecurity."

So does your interpretation of 5(n) agree with the Third Circuit's interpretation or does it differ in some way?

MS. VANDRUFF: We are building on the Commission's interpretation of Section 5(n), which I think is entirely consistent with the unfairness statement.

COMMISSIONER OHLHAUSEN: And is that interpretation you are relying on from Commissioner Wright's decision denying respondent's motion to dismiss?

MS. VANDRUFF: That's correct, Commissioner Ohlhausen, yes.
COMMISSIONER OHLHAUSEN: I have a question about that.

MS. VANDRUFF: Yes.

COMMISSIONER OHLHAUSEN: In that opinion, the Commission says that occurrences of actual data security breaches or actual, completed economic harms are not necessary to substantiate that the firm's data security activities caused or are likely to cause consumer injury and thus constituted unfair acts or practices, and then it cites the unfairness statement, which says what is substantial injury: small harm to a large number of people or raises a significant risk of concrete harm.

So is it your contention that a significant risk of concrete harm equals substantial injury? That's correct?

MS. VANDRUFF: That's correct.

COMMISSIONER OHLHAUSEN: But is it also possible that when Congress interpreted the unfairness statement and recast it in Section 5(n) -- it moved things around, it reversed the order of some of the prongs -- that a significant risk became likely to cause and concrete harm became substantial injury? Is that reading incorrect in some way or not in accord with what Congress said about Section 5(n) or what the unfairness
statement said?

Do you see what I'm saying?

MS. VANDRUFF: No, I understand the question, Commissioner Ohlhausen.

And what I would say is that we don't think that the law has changed in any way since January of 2014 and since Commissioner Wright's opinion on behalf of a unanimous Commission requiring the Commission to change the law with respect to significant risk of concrete harm, but the alternative formulation that you suggest, which I think is that likely means significant risk, would not affect the outcome in this case, as the record demonstrates, because complaint counsel has shown that LabMD's practices have caused a significant risk of concrete harm whether you characterize that harm as causing substantial injury or being likely to cause substantial injury.

COMMISSIONER OHLHAUSEN: Thank you. And that leads us to another question.

So assuming we're judging whether LabMD's actions were likely to cause substantial injury, what type and amount of evidence would meet this standard? Is it a risk analysis, meaning that you need the evidence of both probability of potential harm and magnitude of potential harm, and does the record have
that kind of evidence?

MS. VANDRUFF: So I think what you're asking is keyed off of the briefing from respondent about what likely --

COMMISSIONER OHLHAUSEN: Well, I'm just trying to interpret if we have to apply likely to cause substantial injury, which is the statutory language --

MS. VANDRUFF: Yes.

COMMISSIONER OHLHAUSEN: -- what type of evidence would meet that standard?

MS. VANDRUFF: Right.

COMMISSIONER OHLHAUSEN: And where would we find that in the record?

MS. VANDRUFF: Right.

Well, the term "likely" I don't think there's any question is ambiguous because it is open to multiple interpretations. And if given the interpretation that you've offered, which again is not, in complaint counsel's view, the better reading of the statute -- the better reading of the statute, as we've offered in our briefing, is that significant --

CHAIRWOMAN RAMIREZ: Counsel, let's just put aside what "likely" means. Let's just take your position that the data security practices in this
case created some increased or undue risk of exposure of 
sensitive information. Let's just -- just focus on 
that, this concept of risk.

MS. VANDRUFF: Yes.

CHAIRWOMAN RAMIREZ: And just to 
reframe the question so that you focus on what I 
think we all care about --

MS. VANDRUFF: Okay.

CHAIRWOMAN RAMIREZ: -- so what evidence 
establishes that the practice -- security 
practices -- were what created that enhanced risk 
or increased risk?

MS. VANDRUFF: I'd be delighted to address that 
question.

CHAIRWOMAN RAMIREZ: I believe that's what you 
were trying to get at.

COMMISSIONER OHLHAUSEN: That is what I'm trying 
to get at.

Putting aside the statute versus the 
unfairness statement and how that may have been 
one translated into the other, what evidence do 
we have that --

MS. VANDRUFF: Well, we presented evidence of 
multiple, systemic and serious failures of data security 
at LabMD that exposed 750,000 consumers' --
CHAIRWOMAN RAMIREZ: So walk us through just the top data security practices that --

MS. VANDRUFF: I will.

CHAIRWOMAN RAMIREZ: -- you think were --

MS. VANDRUFF: And can you put our first slide up on the screen.

CHAIRWOMAN RAMIREZ: And as you go through those, I think one question that respondent has raised is from what time frame should we even be looking at this and against what benchmark are you comparing what LabMD did as compared to what you would deem to be reasonable and appropriate security measures.

MS. VANDRUFF: Right.

The testimony in this case and -- and the record evidence I should say -- this is not limited exclusively to our expert witness, but, rather, the testimony in this case is that LabMD's failures spanned really the period, and we're not limited in any way to a narrow time period, as we addressed in our briefing. A suggestion to the contrary is belied by the --

CHAIRWOMAN RAMIREZ: What's the relevant time frame?

MS. VANDRUFF: The time period is from 2005 really through the present.

Now, some of the practices ended in 2010, as we
address in our briefing and in our findings of fact, but many continue through the present. And we certainly contend that LabMD's unlawful data security practices continue through the present and that relief is necessary to protect consumers from harm.

So because my time is limited, I'd like to address the top three data security failures.

And those would include, at the outset, first, that LabMD did not implement any recognizable password policy and for years permitted weak passwords on its workstations, servers and computers in physician offices.

And when I describe these passwords as weak, I'm not splitting hairs between 12 and 14-character passwords. Instead, by way of an example, LabMD permitted many of its employees to use "LabMD" as their password.

Even LabMD's former IT director acknowledges that its password practices were poor. That's his testimony.

The company could have checked for passwords, for strong passwords, and it chose not to.

Second, LabMD did not use available measures to prevent or detect unauthorized access to personal information.
Until at least late 2010, many employees had the ability to download and install any software they wanted to onto their work computers, including unauthorized programs. The danger of this hole in security is starkly demonstrated by the fact that an employee downloaded LimeWire onto her workstation in 2005, but LabMD utterly failed to discover it for years.

COMMISSIONER McSWEENY: So can you just clarify that for me?

MS. VANDRUFF: Sure.

COMMISSIONER McSWEENY: When was the LimeWire program installed? In 2005?

MS. VANDRUFF: That's correct.

COMMISSIONER McSWEENY: Okay. And how long is complaint counsel alleging it remained undetected?

MS. VANDRUFF: It was not detected until May of 2008.

COMMISSIONER McSWEENY: And how was it detected?

MS. VANDRUFF: It was detected when LabMD received a phone call from Tiversa.

COMMISSIONER McSWEENY: And was it detected, then, because there were programs in place to monitor whether outside software was installed on computers? Or was it detected by a physical inspection?
MS. VANDRUFF: It was -- no. It was detected -- the testimony is that it was detected when LabMD undertook to discover whether or not the reported incidence of peer-to-peer software being installed on a computer at LimeWire was in fact true -- excuse me -- at LabMD was in fact true, and so they swept the workstations and discovered that it was.

And if the security problem of allowing employees to download software onto their workstations from the Internet wasn't bad enough, LabMD explicitly directed its employees to store copies of files containing consumers' sensitive personal information onto their workstations.

CHAIRWOMAN RAMIREZ: So, Counsel, just to go back to my question about what the relevant benchmark to use, so how should -- respondent raises an argument about lack of appropriate notice about the standards that they were required to maintain during the relevant time frame. Explain to me how should they have known to have strong passwords during this period, how should they have known that they needed to have particular mechanisms to ensure that a peer-to-peer program like LimeWire would not be installed? What's the relevant benchmark?

MS. VANDRUFF: Well, the relevant standard, of
course, is Section 5(n) in terms of the legal standard in terms of fair notice.

But if your question is how were their IT professionals to have known that they could have used the Windows function to lock down workstations to prevent individuals from downloading software from the Internet, the answer is training and if they had permitted their IT professionals or really any professionals in their system to have undertaken regular training, and that is one of our failures.

CHAIRWOMAN RAMIREZ: But the concept of reasonableness has to be measured against something, right, so what's the benchmark?

So understanding that you want your employees to be trained appropriately as to the appropriate standards. Where do we get those standards, and where are they reflected in the record?

MS. VANDRUFF: So in the record, our data security expert, Professor Hill from Indiana University, describes a number of free resources that were available.

So, for example, written data security policies, examples of those were available as early as 1997, and they were not used by LabMD until -- until 2010.
And so that is but one example, but the record is replete with examples throughout the time period of LabMD failing to use available resources to secure its network reasonably to protect the sensitive personal information on its network from unauthorized disclosure.

COMMISSIONER OHLHAUSEN: Counsel, assuming that they failed to take these precautions, what evidence is in the record about the probability of the harm or the potential harm that consumers might suffer from these failures and the magnitude of that harm?

MS. VANDRUFF: We presented -- I'm glad you raise that question, Commissioner Ohlhausen, because I would like to turn my attention, if I may, to the evidence that complaint counsel presented of the -- the record evidence that LabMD's failures caused or were likely to cause substantial injury.

And the record evidence does establish that LabMD's multiple, systemic and serious data security failures caused a significant risk that sensitive personal information over 750,000 consumers would be disclosed without authorization.

The record -- there are three discrete concrete harms that are at issue.
First is identity theft. The record establishes that consumers suffer out-of-pocket losses and lost-time harms following identity theft. And this risk is not abstract, as I discussed earlier this afternoon. The LabMD documents seized from identity thieves in Sacramento make concrete that identity thieves value the kind of information LabMD collected.

The second risk of concrete harm is medical identity theft. The record establishes that consumers suffer a wide variety of harms from medical identity theft, which would burden consumers with financial costs and serious threats to health. And in addition, unlike identity theft, there's no central medical identity bureau where a consumer can set a medical fraud alert, making remediation difficult.

Third, a disclosure itself constitutes a concrete harm under Section 5. Sensitive health information is the type of personal information the Commission has sought to protect since its earliest data security case in 2002, Eli Lilly, through its fiftieth data security settlement in GMR Transcription Services.
COMMISSIONER McSWEENY: So can I ask a question about this?

MS. VANDRUFF: Yes.

COMMISSIONER McSWEENY: Are you saying that there's injury from any exposure of any health information?

MS. VANDRUFF: Not -- not necessarily, but the kinds of information that could be stigmatizing. In this case, there was information about testing for HIV, testing for cancer, testing for other kinds of potentially stigmatizing conditions.

I can imagine that there could be health information that might be benign, but those aren't the facts here. There are facts here -- the facts that are in the record here are information that consumers would necessarily want to be maintained as confidential.

COMMISSIONER OHLHAUSEN: Counsel, how does that square with the unfairness statement, which talks about substantial injury mainly involving monetary harm, but emotional impact not ordinarily making a practice unfair? How would you apply that to the disclosure of the medical information that was disclosed in this case?

MS. VANDRUFF: While I -- the unfairness statement certainly talks about the principal injury
being economic, I think that it recognizes that there
would be narrow cases, again, not trivial or
speculative or emotional harms but -- but the kinds of
concrete harms where consumers, you know, again suffer
the kinds of harms that result from the disclosure of
the most sensitive kinds of information, like being
tested for HIV or cancer. I do think that that is
different in kind and again has been recognized in our
own cases before the Commission.

CHAIRWOMAN RAMIREZ: What's the most closely
analogous case? You mentioned Eli Lilly.

MS. VANDRUFF: GMR Transcription from 2014 I
believe it is, yeah, August 2014, which was our
fiftieth -- the Commission's fiftieth data security
settlement by unanimous Commission.

COMMISSIONER OHLHAUSEN: One other
question.

You talked about the evidence of the
magnitude of the harm.

What evidence do you have that these practices
would -- were likely to lead to these harms, that the
data security, if they had these kinds of practices,
how likely was it that consumers' information
would be exposed or released?

MS. VANDRUFF: Well, the -- it was -- the
testimony -- well, I should say that our data security expert, Professor Hill, demonstrated that the practices of LabMD increased the risk of unauthorized disclosure of information. And paired together with the evidence of our identity theft experts, we have established that those harms -- that there was an increased risk of those concrete harms.

Now, respondent --

COMMISSIONER McSWEENY: Can I ask one more question? I just want to clarify something about the data security practices you identified here.

MS. VANDRUFF: Yes.

COMMISSIONER McSWEENY: To the extent that they were tracking what was on employees' computers that were attached to the network, were they doing that through automated tools or were they doing that through physical inspections or random inspections?

MS. VANDRUFF: The record is that through 2010 at least that the principal means of monitoring the network and the software that appeared on employees' computers was through what they called walk-around inspections, and the record is further --

COMMISSIONER McSWEENY: What is a walk-around inspection?
MS. VANDRUFF: So -- and the record is further that they would basically check in when computers weren't working properly, and so if you had trouble printing, you would call the person at the IT desk, and he would come over and fix it. But it wasn't any kind of routinized process, so it was very reactive, if you will.

COMMISSIONER McSWEENY: And were -- I think you're out of time.

MS. VANDRUFF: And I'm out of time.

CHAIRWOMAN RAMIREZ: Go ahead. We can always go over a little bit.

COMMISSIONER McSWEENY: Were physicians who were sending information in to the network doing that without encryption tools or data security tools? Is that right?

MS. VANDRUFF: The evidence is that it was over a file transfer protocol and it is -- we don't contend that it was unencrypted. It is -- there's -- the record is mixed about exactly how protected that was, but that is not a contention that complaint counsel makes.

COMMISSIONER McSWEENY: So the use of the file transfer protocol during this period of time isn't alleged by you to be an unreasonable security practice.
MS. VANDRUFF: There were vast quantities of data being transferred, and there were issues about the configuration of the firewall, but I don't think that encryption is the concern.

COMMISSIONER McSWEENY: Thank you.

CHAIRWOMAN RAMIREZ: So just one more question for you, so let me just go back to one of Commissioner Ohlhausen's questions about what evidence establishes the likelihood of harm or probability of harm, as she put it.

The ALJ was very persuaded by the absence of a concrete example of ID theft in the time that had elapsed between both the discovery and exposure of the 1718 File as well as the Sacramento documents.

What role does this, what one could call as a shorthand ex post evidence, have in the way that we evaluate whether data practices were likely to cause substantial injury?

MS. VANDRUFF: I don't believe it has a role, Madam Chairwoman.

CHAIRWOMAN RAMIREZ: Is it relevant at all?

MS. VANDRUFF: I don't believe it is relevant, particularly in the case of identity theft, because, of course, the ability of a consumer to tie up the incidence of a particular breach to a particular
experience of identity theft is attenuated at best and impossible in most circumstances, particularly here where no consumer has received notice that the information contained in the 1718 File was exposed on the peer-to-peer network, so there's no ability whatsoever for the 9300 consumers whose information was contained -- was exposed on the peer-to-peer network for eleven months to even know that there's a possibility that --

CHAIRWOMAN RAMIREZ: Okay. Sure. And I think what you're saying is that the ALJ -- that what he required, which was showing that one of the 9300 people who had been -- whose information had been exposed in the 1718 File, for instance, the fact that there's no evidence of one of those people having suffered medical ID theft, that is of no relevance.

But the fact that there was the exposure of the 1718 File, the fact that the Sacramento documents were found in the hands of identity thieves, of what relevance is that to the analysis of whether or not the data security practices were likely to cause substantial injury?

Does that tell us anything about whether or not the data security practices were reasonable or unreasonable?
Ms. Vandruff: Right. I think that the fact of those exposures does suggest that -- I mean, there were incidents of unauthorized disclosure, and so I think that that does point us to -- it shows that the increased risk was further magnified and that the consumers --

Chairwoman Ramirez: So it is relevant.

Ms. Vandruff: It is absolutely relevant, yes. I'm sorry. I thought you were asking a different question, Madam Chairwoman.

Chairwoman Ramirez: I probably made it too convoluted.

Anyone else?

Commissioner McSweeny: Sorry, I have one more question.

Ms. Vandruff: Yes.

Commissioner McSweeny: How do you respond to LabMD's argument that this investigation was triggered by the receipt of the 1718 file from Tiversa, but that Tiversa's actions in obtaining the file were unlawful?

Ms. Vandruff: Tiversa is a witness upon whom complaint counsel does not rely in this appeal to the Commission and upon whom complaint counsel did not rely in its briefing, post-trial briefing before the Administrative Law Judge.
Its relevance in this appeal in the Commission's de novo review is as a third party that provided a tip to the Commission. The tip was that LabMD was disclosing sensitive personal information on a peer-to-peer network, a tip that proved to be true.

The Commission staff investigated that lead and corroborated it with information provided by the respondent.

COMMISSIONER McSWEENY: Can I just ask --

MS. VANDRUFF: That is the end of the inquiry.

COMMISSIONER McSWEENY: Can I just follow up on this?

MS. VANDRUFF: Yes.

COMMISSIONER McSWEENY: Is it the exposure on the peer-to-peer network of the LabMD file that I should be weighing here? Or is it the presence of LimeWire on the employee computer that went undetected for two-plus years?

MS. VANDRUFF: Both, Madam Commissioner.

COMMISSIONER McSWEENY: Okay.

COMMISSIONER OHLHAUSEN: I have a question about the peer-to-peer.

There's evidence that one entity accessed or was able to access that file on the peer-to-peer.
Do we know whether anyone else was able to
download or access the information?

MS. VANDRUFF: The record evidence is from --
from LabMD's own witness, Richard Wallace, that he was
able to use an ordinary computer and an ordinary
peer-to-peer client and download the 1718 File. He
downloaded it on behalf of his then employer, Tiversa,
who shared it with a researcher at Dartmouth University.

We don't have evidence of whether it was
otherwise shared because the hard drive on which the
LimeWire software was installed and the file -- from
which the file was being shared was destroyed during a
LabMD forensic investigation, so that is information
that complaint counsel was not able to obtain during its
investigation.

COMMISSIONER OHLHAUSEN: So if I understand what
you're saying, we know it was capable of being accessed
that way and we know somebody did access it that way.
We don't know whether others did because the hard drive
had been damaged.

MS. VANDRUFF: Correct.

COMMISSIONER OHLHAUSEN: Okay. Thank you.

CHAIRWOMAN RAMIREZ: Thank you, Counsel.

MS. VANDRUFF: Thank you.

CHAIRWOMAN RAMIREZ: You may begin when you're
ready, Mr. Lechner.

MR. LECHNER: May it please the Chairwoman and Commissioners.

I would like to start with just some basic information first.

Initially, Dr. Hill unequivocally testified that the physical security at LabMD was adequate, so statements to the contrary are not supported in the record.

With regard to the Sacramento files, there is absolutely no evidence that they came off of the LabMD system, computer system, none at all, nothing to support that. They were found in a house that was raided because of a -- I believe it was utility theft, and maybe it was electric or gas theft, and they found these documents there by questionable individuals who pleaded nolo contendere to a charge of identity theft, but that's not established in the record either.

So there's nothing with regard to the Sacramento documents to link it to the system. There is simply no basis to suggest that that supports any evidence of a --

CHAIRWOMAN RAMIREZ: So, Counsel, you heard complaint counsel argue that the case is about more than just electronic security and more than just
computer security and also includes physical security. I take it you take issue with that?

MR. LECHNER: Well, sure, I do. There's nothing in the complaint that says that. I mean, we've been looking at a situation here that's been changing with the filing of that complaint right to the very moment now. Now we're told, although there's been testimony that at least there's one period of time from June of 2007 to May of 2008 is the relevant period, then we were told I believe it was 2005 to 2010, that six-year period, and now we're told it's a twelve-year period from 2005 to 2016. It's a moving target.

Dr. Hill has testified unequivocally. She offered no testimony beyond 2010. There is nothing to suggest anything beyond 2010. To expand it is simply not supported in the record and argues off the record and off the complaint.

CHAIRWOMAN RAMIREZ: Is it possible that the Sacramento documents came from any other source other than LabMD?

MR. LECHNER: I don't know where they could come from. There's been no evidence. I can't speculate where they came from. It's not my burden to disprove that. It's their burden to prove it, and they haven't
offered any evidence, other than speculation, which
really I think is the key to their case. It's
speculation.

They -- I believe it was Commissioner Ohlhausen
who asked whether a likelihood of substantial injury, if
that's established, or a likelihood of raising a
concrete harm, the possibility of concrete harm, equals
an injury. And if I heard correctly -- and I think I
read it in the brief -- they argue it does. That makes
no sense.

CHAIRWOMAN RAMIREZ: Okay. Tell us what the
appropriate legal standard is.

MR. LECHNER: Well, I can tell you what the
statute says, and then we can talk about where they fell
short.

The statute is clear, Section 5(n) is clear that the
Commission cannot find something unreasonable unless --
that word "unless" is prominent -- it finds that there
was a harm that was caused in the past or likely that
the conduct would cause substantial injury.

"Likely to cause substantial injury" is
prospective - in the future. "Likely" equals probable.
There's no question about that. It is not ambiguous.

CHAIRWOMAN RAMIREZ: Let me start with the
actual harm prong of the unfairness standard.
MR. LECHNER: Sure.

CHAIRWOMAN RAMIREZ: Isn't there actual harm here? Isn't the exposure of the 1718 File itself harm?

MR. LECHNER: Exposure to whom?

CHAIRWOMAN RAMIREZ: To, at a minimum, Tiversa.

MR. LECHNER: Well, Tiversa stole it, and they tried to monetize it and they lied. There's no question that the people from Tiversa lied, except for Wallace, but the Commission has tried to backpedal away --

CHAIRWOMAN RAMIREZ: Well, Tiversa didn't steal the document; correct?

MR. LECHNER: Well, they broke --

CHAIRWOMAN RAMIREZ: Hold on.

MR. LECHNER: I'm sorry.

CHAIRWOMAN RAMIREZ: Tiversa accessed the document via a peer-to-peer program that permits sharing of files; isn't that true?

MR. LECHNER: Well, I'm not sure about that. They were talking about using their Eagle Eye (sic) program to break into it, which is supposed to be a lot more sophisticated than normal peer-to-peer.

But in any event, they were not authorized. They broke into it, and they broke into it for one purpose, to try to blackmail the people that they broke
into, in this instance LabMD, to paying them money. And when they didn't, then they partnered up with the FTC and tried to have the FTC do their dirty work, as Boback talked about, wait until you see what happens next.

COMMISSIONER OHLHAUSEN: Counsel, let me ask you, assume that we agree with you that Tiversa was a bad actor.

MR. LECHNER: Yes.

COMMISSIONER OHLHAUSEN: How are we to evaluate LabMD's data security practices that enabled this bad actor to obtain sensitive information about patients?

MR. LECHNER: Well, there's no testimony, no expert testimony, to establish that that in point of fact is what happened.

You talk about many times, as the Chairwoman mentioned, what is the standard. Well, the standard, as was pointed out, changes. And in your own memorandum of law dismissing our motion to dismiss, you pointed out that this is a rapidly changing technology.

So when Dr. Hill testified, she did not offer any testimony as to what the standard was from time to time. And we know that these standards changed from 2005 to 2010, yet there was no basis, no benchmark, if you will, as that term was used here this morning. But
there has to be that in order to demonstrate, number
one --

CHAIRWOMAN RAMIREZ: So the use of strong
passwords, you don't think that that was established as
of 2005 or 2010? Is that what your position is?

MR. LECHNER: Well, I think we're looking at in
retrospect right now what we know eleven to twelve years
later as to the strength of these passwords. And when
you go on a commercial site and you open up a site -- if
I could just --

CHAIRWOMAN RAMIREZ: Go ahead.

MR. LECHNER: I'm sorry -- they sometimes open
back and say this is strong or this is weak, this
password. They did not do it back in 2005. But you
can -- you could pick out one or two of these things and
say, in my view, this was not strong, but what
Professor Hill did not do is establish how that standard
was deviated from at the time in question from time to
time during that six-year period, and that's just one
instance there.

They had the obligation to prove that. These --
these allegations here have to be proved by expert
testimony. It can't be an ipse dixit from the
Commission that they see something that they don't
like, and therefore there's a problem, and therefore
there's a harm. This is speculation based upon speculation.

COMMISSIONER OHLHAUSEN: So, Counsel, you're saying that you looked at the standard of reasonableness at the time that LabMD was operating under its various security choices there, so you're not looking from the ten-year vantage point back but at the time.

MR. LECHNER: Yes.

COMMISSIONER OHLHAUSEN: You're saying that there's no expert testimony or no information about what would have been reasonable data security practices in 2005; is that correct?

MR. LECHNER: With regard to --

COMMISSIONER OHLHAUSEN: Or 2005 to 2010.

MR. LECHNER: That's precisely what I'm saying.

And another point, just as an aside for one moment just to support that, more than thirty times, more than thirty times, Professor Hill was asked if she formed an opinion about, for example, X or Y. Professor Hill said, "Yes." The next question more than thirty times was: "What was your conclusion?" She responded, "My conclusion is." That testimony is incompetent and can't be considered.
Case law is clear that an expert cannot offer legal conclusions. That is for the trier of fact. That was wrapped up at the end of this testimony when the professor was asked, Based upon all -- on all of your opinions, do you have a conclusion -- conclusion? Excuse me. Yes. What was it? My conclusion is, and then she offered that conclusion.

That testimony, frankly, is wrong. The counsel was warned about that by the ALJ right in the middle of that testimony and continued along those lines.

But to go back to the absence of the standards here, in not one place does Professor Hill talk about a deviation from established standard and how that standard changed from time to time to time, and we have a six-year period when the standards are changing, as was pointed out by the Commission in their order dismissing the motion to dismiss. That's a given, yet there's no --

CHAIRWOMAN RAMIREZ: Don't LabMD's own policies with regard to its network security tell us something about what was considered reasonable at the time?

MR. LECHNER: Well, yes. There was a policy there that these computers were not to be used for personal use basis. They couldn't go on and look at ESPN. They couldn't go on and use it for --
CHAIRWOMAN RAMIREZ: And you don't think it would be reasonable for a company to have some form of monitoring to ensure that those policies were followed?

MR. LECHNER: Well, there was testimony that there was monitoring there, but that's the question, why -- and there was no opinion as to what was wrong with that monitoring compared to what the baseline was from time to time.

There's just a broad brush. There's no attempt to segregate this and look at it from period to period, nor to look at it from whether paragraph 10(a) or right through paragraph 10(g) and break it out seriatim as each of those moved on from year to year to year.

COMMISSIONER McSWEENY: Let me just back up because I am confused about this argument that there were no standards in place during this period of time that you could follow.

MR. LECHNER: I'm sorry?

COMMISSIONER McSWEENY: Aren't we talking about HIPAA-covered documents, medical records, and hopefully state standards here as well?

MR. LECHNER: Well, that's just the point. Professor Hill said she was not familiar with HIPAA. Professor Hill did not link any standard to this industry in particular or to this business in particular, and the
reasonableness demands both.

You cannot use a broad brush with regard to the industry in general. What industry would it be? The security industry? Would it be the computer industry? Or is it the industry of the accumulation of medical data for legitimate purposes, as LabMD was involved in?

But that's another point that was not done here. There are no base standards with regard to the particular company involved. And as the Commission pointed out, that's what has to be done in order to look at what reasonableness is. It's based upon the circumstances.

What are the circumstances? The company in question, the size of it, what it does, how it does it, what its business involved, and over what period of time are we looking at it and how did those standards change.

There was no testimony at even the basic that the standards remained the same the whole time.

And I think it was acknowledged, again to go back to your order on the motion to dismiss, that this technology is rapidly changing, if not day to day, at least much more quickly than one would expect.

CHAIRWOMAN RAMIREZ: Well, what I think the Commission stated in its decision was that it's a
company's obligation to be constantly evaluating its risks and placing appropriate security measures in order to protect the information that's contained, so that's the question that we're trying to determine, whether LabMD did that, correct, so --

MR. LECHNER: And my point is, Madam Chair, is that that's not my obligation to prove. My obligation is to disprove I had notice of it, but there's no testimony establishing what the standard was that we deviated from from time to time with regard to each of these particulars. There was general conclusion that was offered to each of these areas but not an opinion based upon a reasonable degree of probability.

CHAIRWOMAN RAMIREZ: Can any conclusion be drawn from the existence of LimeWire on the LabMD network? Does that tell us anything about the reasonableness of the data security practices?

MR. LECHNER: Well, it's interesting. The position of this body was that P2P networking and programs were neutral. That was testified to in front of a Congressional commission in July of 2007, that P2P file sharing is neutral technology.

After that, the FTC position didn't change until after 2008, and the FTC didn't give any notice of warning businesses about the so-called dangers of P2P
until after it commenced the action against LabMD in January 2010, so even the FTC's conduct here --

CHAIRWOMAN RAMIREZ: I've taken a look at that testimony. I don't read it the way that you do, and so I understood that the agency in fact was educating both consumers and businesses at that time about the risks, the potential risks, of peer-to-peer technology, and encouraged businesses to evaluate those risks.

COMMISSIONER McSWEENY: Let me frame that question slightly differently, if I may.

CHAIRWOMAN RAMIREZ: Go ahead.

COMMISSIONER McSWEENY: Is the existence of unsanctioned, undetected software that was installed by an employee on a computer something that we should take into account in assessing whether reasonable security practices were in place?

MR. LECHNER: By itself, no. It doesn't mean anything. Because, number one, there's been no -- what has to be done here -- just for argument sake, let's just take that proposition as a given. All right? But then the question is: Did that cause any harm? The answer is no here. There's no allegation that any harm was caused. The allegation is that it was likely to cause substantial injury.

Now, there's no testimony with regard to the
probability of that -- assume for argument position --
was likely to cause substantial injury.

Now, if you wanted to use the new standard that
they are trying to allege now after the fact that they
did not allege until after their post-trial briefing that
we should read likely to cause substantial injury as
likely to raise a substantial risk of -- risk of
substantial -- of a concrete harm, that's even more
difficult to prove, because then you need expert
testimony of the likelihood that it's going to cause it,
what -- what the risk is, how the risk increased from
what to what, and we --

CHAIRWOMAN RAMIREZ: Counsel, if I may, and
just going back to this issue of what one can infer
from just even the existence of the LimeWire program
being placed on a computer, there is testimony from
Mr. -- Dr. Shields about the ease with which someone
could access files that have been made accessible via
peer-to-peer programs. Isn't that evidence
showing that that creates a risk of exposure of
sensitive information?

MR. LECHNER: Well, first of all, the LimeWire
was taken off promptly, as you know, back in 2008.
There's no testimony from him as to what period
of time he's talking about. We are just using this block
of time. Again, I go back to the same position that you
cannot look at this as a monolithic block with standards
not changing.

And third of all, it's speculative because
there's not one incident either from the Sacramento
documents nor one incident from the documents that were
taken by Tiversa without authority that anyone saw these
documents except Tiversa, and they gave it to this
professor and the FTC, who gave it to experts. Nobody
else saw this.

COMMISSIONER OHLHAUSEN: Counsel, we know that
Tiversa did access the file through peer-to-peer. We
don't know whether anyone else did. Is that correct?

MR. LECHNER: Well, we do know this, that LabMD
had two of its employees use their home computers and
tried repeatedly to use file-sharing programs and were
not able to locate it. That's in the record.

COMMISSIONER OHLHAUSEN: But can you explain
why they weren't able to determine that from the
hard drive with the forensic audit?

MR. LECHNER: I don't know. That's not my
burden. I simply don't know. I can't speculate as to
that, which is again --

CHAIRWOMAN RAMIREZ: What happened to that
computer? It's unclear from the record what happened to that computer.

MR. LECHNER: I have no idea.

CHAIRWOMAN RAMIREZ: There's nothing in the record about --

MR. LECHNER: Not that I'm aware of.

COMMISSIONER McSWEENY: And it's also, I think, not totally clear what other files might have been accessible through LimeWire on the computer. Is that right?

MR. LECHNER: Well, again, that's speculation. You're correct. That's total speculation. There's no factual testimony on that, no expert testimony on that, rank speculation, yes, as far as that's concerned.

But to go back to the standard that's involved here, we do have a migration of this right now from likely to cause substantial injury to likely to raise a significant risk of concrete harm. I suggest to you that if you're going to use the second one, you need an expert witness to opine as to what "likely" would mean, what "substantial" and what "risk" means and what "concrete harm" means.

Concrete harm certainly, as -- if you look at the footnote in the fairness statement, does not mean anything that could -- if somebody feels bad or has an
emotional problem. "Concrete" means, what has been
decided in every case that's been brought so far, an
actual injury, monetary injury.

Now, I'm not suggesting that you have to have
an actual injury to have a violation of 5(n), but you
need to prove -- and it's in the disjunctive -- either
the actual injury causes or it's likely to cause
substantial risk of concrete harm or raise that, so you
need that benchmark in there.

COMMISSIONER OHLHAUSEN: So is it your position
then under Section 5(n) that complaint counsel has to
establish the precise calculable risk of injury?

MR. LECHNER: What counsel has to do, just like
in the tort field, as this Commission has recognized,
this is an evolving standard, as is done in -- for
contracts and for torts, likewise here, too, that even
though there are no articulated standards per se out
there, that there would be testimony that would be
offered that this is the standard, that there's a
deviation from the standard, as a result of that
deviation that harm has been caused. You see that every
day in medical malpractice cases.

COMMISSIONER OHLHAUSEN: So you're not saying that
complaint counsel would have to show that there was a
52.3 percent --
MR. LECHNER: They have to show a probability.

No, I'm not suggesting it has to be numerical, but it has to be probable.

COMMISSIONER OHLHAUSEN: And what would "probable" mean? Would it mean --

MR. LECHNER: More likely than not.

COMMISSIONER OHLHAUSEN: So if a practice has a 25 percent probability of resulting in a loss of a million dollars --

MR. LECHNER: That's not probable.

COMMISSIONER OHLHAUSEN: -- that wouldn't be expected to be likely to cause substantial injury?

MR. LECHNER: That would be possible. That would not be probable.

COMMISSIONER OHLHAUSEN: And then how does that square with, say, for example, International Harvester, where the Commission interpreted --

MR. LECHNER: Well, that case is distinguishable. There were actual injuries in that case. There were actual injuries in that case. That's entirely different from this case where there are none.

In that case, there were actual injuries, and they were talking about it in light of those actual injuries there, so that probability was not required there because you had an actual injury.
COMMISSIONER OHLHAUSEN: So you're saying that "likely" means has to be probable.

MR. LECHNER: And that's what the case law says.

Absolutely.

COMMISSIONER OHLHAUSEN: But wouldn't you say that at least the statute is ambiguous on that?

MR. LECHNER: No.

COMMISSIONER OHLHAUSEN: Then why doesn't it say "probable"?

MR. LECHNER: Because likely is the equivalent of probable. You look up any case in the Eleventh Circuit --

CHAIRWOMAN RAMIREZ: So what cases are you relying on?

MR. LECHNER: I'm sorry?

CHAIRWOMAN RAMIREZ: What cases are you relying on when you say that --

MR. LECHNER: Oh, I can get you the cases. I can make that representation to you. I know that as a fact that likely is the substantial equivalent of probable. Likely and probable means more likely than not. It does not mean possible. Possible means not impossible. Likely means more likely than not.

And that's the question for the trier of fact, does it come to that? I am not suggesting that there
must be a numerical grade attached to this. No. The
expert has to testify that in her opinion, it's more
likely than not or probable that as a result of this
conduct, there is a chance of -- or, rather, a risk of
increased -- of substantial injury.

COMMISSIONER OHLHAUSEN: So what do we make of the
unfairness statement's discussion of avoiding
speculative injuries?

MR. LECHNER: Well, that's just it. That's why
it has to be probable.

COMMISSIONER OHLHAUSEN: So you say that if
something is nonspeculative, it means it has to be --
have a greater than 50 percent chance of occurring.

MR. LECHNER: Yes. And that's what the case law
says. That's what every case law in negligence talks
about, whether it's medical malpractice, architectural
malpractice --

COMMISSIONER OHLHAUSEN: But we're not
interpreting negligence torts here; right?

MR. LECHNER: But my point is, you used the
example of this standard evolving the same way the
definition of negligence has evolved, the same way
negligence standards have evolved. That's part of your
opinion in dismissing the motion to dismiss, that that
is an evolutionary process.
And because this Commission has not issued
standards -- and issuing standards is a long process.
There's public comment. People read it. You get input
from the industry. People are aware of what's going
on.

So the courts have allowed, in lieu of that, to
have this evolutionary process in the courts as to what
this would be, and that's what you have articulated in
the motion to dismiss. This is an evolutionary
process.

Now, to have that process move along absent
standards, there has to be some gradual
determination as to what happens from case to case
because, as you've said, it is a case-by-case
development.

In order to have that, there has to be the
establishment of standards for the period of time, for
the company in question, for the industry, and if that
period of time varies over a number of years, at least
the testimony that it's the same standard for all these
years or how it's changed, that there's a deviation from
that standard, and it's because of that deviation, as is
in this case, more likely than not or probable that that
conduct that has been called to be unreasonable has
increased the risk of substantial harm.
COMMISSIONER McSWEENY: Can I focus on a period of time here for just a second, because I am a little confused about what period of time we're talking about.

In your brief, you focus, I think, on the 2007 to 2008 time frame. Dr. Hill's testimony focuses on 2005 to 2010. Complaint counsel has mentioned that you still have a lot of sensitive information and some ongoing issues, in their view, surrounding how that information is being protected.

What steps is LabMD taking at this point to ensure that highly sensitive information is being protected? And in your view, what is the relevant period of time that we should be considering?

MR. LECHNER: Well, it's my understanding that LabMD is out of business now.

COMMISSIONER McSWEENY: But it still has a huge amount of patient information.

MR. LECHNER: I don't know how much it has left, but it's not doing business right now as a result of the expense and the problems with this case.

That's one of the problems. You know, when the Commission brings something like this, a lot of these cases end up --

COMMISSIONER McSWEENY: Let's back up for just a second.
MR. LECHNER: I'm sorry?

COMMISSIONER McSweeney: What is the relevant period of time?

MR. LECHNER: The relevant period -- I'm sorry. The relevant period of time I'd suggest to this body is May of 2007 to -- June of 2007 to May of 2008. I know that there's testimony offered to through 2010, but there is absolutely nothing beyond 2010 other than rank speculation and argument. At worst for us it's to 2010.

But more precisely, it's to 2008 because the Sacramento documents are a red herring in this case. And the only thing that we're talking about here is the 1718 File, which there is no testimony that it was viewed by anybody other than Tiversa, Tiversa's professor I think in Dartmouth, the FTC and the people to whom the FTC gave it. That's the only testimony in this case.

COMMISSIONER Ohlhausen: But doesn't that go back to the idea that you have to show actual harm versus likely harm?

MR. LECHNER: Yes. Well, that's the point. You can either show actual harm, and if you can't show that, we'll concede that the alternative, the "or" in the disjunctive there, you know, that the alleged
unreasonable conduct likely increased the risk of substantial injury or they're trying to cause now concrete injury.

COMMISSIONER OHLHAUSEN: And what about the idea that exposing someone's private health information for a stigmatizing condition is in itself a harm?

MR. LECHNER: You know, that by itself, that can't be. That just can't be because there's no injury in that. There's no substantial injury, as you talked about.

COMMISSIONER OHLHAUSEN: But going to the unfairness statement --

MR. LECHNER: Yes.

COMMISSIONER OHLHAUSEN: -- it says, generally it's monetary harm, but there could be in some circumstances the type of harm that would be if you can show that it would lead to some sort of actual injury.

MR. LECHNER: Right. And that's what they --

COMMISSIONER OHLHAUSEN: Like harassment or something like that.

MR. LECHNER: That's what they would have to show. They haven't showed anybody has even complained, number one, about this, much more that anybody has viewed these documents other than people I've mentioned,
much more that anybody suffered any harassment or any
other type of soft injury. There's been nothing here.
Everything is total speculation.

COMMISSIONER OHLHAUSEN: But what if they showed
that exposing this type of information leads -- likely
leads to those kinds of harms?

MR. LECHNER: But they haven't shown that.

Look at the expert testimony of Kam and
Van Dyke. They used surveys five years after the fact
trying to extrapolate backwards, relying on Boback
testimony extensively. That methodology is completely
wrong. That methodology can't be relied upon.

There's nothing there to demonstrate, even on
the basis that you folks have established in some of
your cases, that the methodology is the first thing that
would have to be looked at. There was none in this case
by either Kam or Van Dyke.

And Professor Hill explicitly testified that she
was assuming harm. She didn't opine as to harm. She
was told to assume harm, so there's nothing from
Professor Hill on that either.

There is an absence of proof in this case, an
utter absence of proof in this case. It's speculative.

COMMISSIONER McSWEENY: If more than Tiversa, the
FTC and the various investigators had viewed the
1718 File, would that be harm?

MR. LECHNER: Well, I don't know. It would depend on the circumstances, as you point out. All the circumstances in a particular case on a case-by-case development have to be considered. And that's something that the trial court would have had to consider, but in this case there was nothing for him to consider. As he pointed out, there was a total failure of proof in this case.

Nobody else looked at it. After all these years, after all of these years, not one person has come forward. Even taking what Professor Kam -- or Mr. Kam and Mr. Van Dyke talked about, the percentages there, not once after seven years has anybody come -- and they were talking about that percentage of each of those instances within twelve months.

COMMISSIONER OHLHAUSEN: Counsel, does your interpretation of Section 5(n) agree with the Third Circuit's interpretation in Wyndham?

MR. LECHNER: Well, it seems to me that's entirely different because there was concrete harm, millions of dollars was run up, and they didn't really focus on what we're focusing on here, so to say that is --

COMMISSIONER OHLHAUSEN: But you're saying the
facts are different, but I'm asking you whether their interpretation of the statute is correct.

MR. LECHNER: I don't recall exactly what they said, but I think they recognized that the FTC has the obligation to prove, in the disjunctive, either actual harm or likelihood of increased risk of concrete harm, if you want to use that secondary standard, which is a deviation from the statute, or likely to cause substantial harm in the future.

COMMISSIONER OHLHAUSEN: So the Wyndham court talks about the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from an investment in stronger cybersecurity, so they're talking about the cost-benefit analysis and considered a number of factors.

So the probability and expected size, how does --

MR. LECHNER: They're talking about probabilities there and they're talking about looking at all of the circumstances. All the circumstances, the company, the timing, the variations from time to time, all that is part of the circumstances.

COMMISSIONER OHLHAUSEN: But aren't you also
saying that if there isn't a showing that there was an actual harm that there's no violation?

MR. LECHNER: No, no, no, I'm not saying that at all. I'm saying it's in the disjunctive. They can show actual harm or they can show a likelihood that would cause a substantial injury.

COMMISSIONER OHLHAUSEN: And if I recall correctly, you're saying that that likelihood has to be greater than 50 percent.

MR. LECHNER: Well, it has to be more probable than not, yes. And by every definition that you've looked at in every case, probability means more than 50 percent.

COMMISSIONER OHLHAUSEN: In unfairness cases?

MR. LECHNER: Well, if you're going to use the word "probability," it can't -- you can't have a 10 percent chance of something happening and to say that's probable, especially in light of the fact of the recognition of this Commission that because those standards were not issued, it's going to be a case-by-case development, we're going to use the protocol that's used in the case and in the courts of this country, and invariably, in every single court, it has never been sustained that the plaintiff has proved his or her case without demonstrating a probability of
a cause -- of the injury being caused by the defendant.

CHAIRWOMAN RAMIREZ: So, Counsel, just to make
sure that I'm clear as to your position, we do know
that the record does establish, the evidence does
establish, that LimeWire was on the computer in LabMD's
network from approximately 2005 through May of 2007;
correct?

MR. LECHNER: Yes.

CHAIRWOMAN RAMIREZ: And we do also know that
the 1718 File was within the files that were accessible
via this peer-to-peer program; correct?

MR. LECHNER: Well, I wonder --

CHAIRWOMAN RAMIREZ: Is that correct?

MR. LECHNER: Well, I just want to challenge
that. I'm not sure it's peer-to-peer. It was their
Eagle Eye (sic) program. Maybe that's a distinction
without a difference. I don't know.

COMMISSIONER McSWEENY: May I just clarify? I
think it was on the computer until May of 2008. Is that
correct?

MR. LECHNER: Yes. Yes. It was an eleven-month
period. Yes, you're right. June of 2007 to May of
2008, the eleven-month period, yes.

CHAIRWOMAN RAMIREZ: So that is correct; right?

MR. LECHNER: It was on there, yes. Yes.
CHAIRWOMAN RAMIREZ: And are you saying that
the availability of Social Security information as well
as sensitive medical information on a peer-to-peer --
through a peer-to-peer program, that that itself is not
either actual harm or likely to cause substantial harm?

MR. LECHNER: That's absolutely what I'm saying,
because if that were the case, there would be no reason
for this trial. There would be no reason. The
Commission through its complaint counsel would have
moved for summary judgment.

As you recognized, there were issues here, there
were fact issues, there were issues with regard to the
expert testimony here. The mere fact that something is
there does not mean by definition it equals an injury.
If there's --

CHAIRWOMAN RAMIREZ: So in your view,
complaint counsel had to establish access, that someone
accessed that file other than Mr. Wallace, in order to
show -- to prevail and show liability here; is that
right?

MR. LECHNER: They would have had to
demonstrate through expert testimony that it was more
likely than not that that one incident itself was
unreasonable and therefore that it was likely to cause
substantial injury in the future, which they didn't do.
CHAIRWOMAN RAMIREZ: Okay. Well, it's not an incident; right? It's this file was available for a period of --

MR. LECHNER: Well, if you want to call that, yes. The eleven-month period, yes.

CHAIRWOMAN RAMIREZ: -- eleven months.

MR. LECHNER: Yes. I agree.

CHAIRWOMAN RAMIREZ: Let me turn to the parts of the unfairness standard, and let's just assume for purposes of argument -- I know that you take issue with this -- that complaint counsel has established either actual harm or a likelihood of substantial injury.

Tell me what your position is about the other prongs of the unfairness standard, that is, whether such harm was reasonably -- would have been reasonably avoidable by consumers or whether it was outweighed by countervailing benefits to either consumers or competition.

MR. LECHNER: Well, as you know, in this case it wasn't addressed because the judge found that there was no injury established or -- and they did not establish a likelihood of substantial injury in the future. But if that were established, then clearly under the statute under 5(n) those other two prongs would have to be addressed. But those other two prongs
are dependent upon the existence of a harm or the likelihood of harm.

CHAIRWOMAN RAMIREZ: So the ALJ -- you're correct, the ALJ did not address those issues in his opinion, but are there -- is there anything in the record on those points?

MR. LECHNER: Not that I --

CHAIRWOMAN RAMIREZ: Is it your position that consumers could have done something to alleviate any unreasonable data security practices on LabMD's network?

MR. LECHNER: I can't address that. I don't know.

CHAIRWOMAN RAMIREZ: You don't know, not one way or the other?

MR. LECHNER: No.

CHAIRWOMAN RAMIREZ: Anything further, Counsel?

MR. LECHNER: Well, let me just really quickly, if I may, just look at my notes just to be sure that I was able to cover the points I wanted to hit.

COMMISSIONER McSWEENY: I do want to circle back on one aspect here -- I understand you don't know what information the company currently has, but should I be concerned about how we can ensure, absent an order, that sensitive information is
appropriately protected?

MR. LECHNER: Well, you know, of course, the --

COMMISSIONER McSWEENY: Assuming I disagree with

the time frame that you put forward.

MR. LECHNER: I'm sorry?

COMMISSIONER McSWEENY: I said, assuming that I

disagree with the time frame that you put forward.

MR. LECHNER: This Commission can offer

guidelines, can offer standards, can establish guides

along those lines here, but may I respectfully suggest

this is not the case to do it because there's not the

factual foundation to do it.

My colleague gave me -- if you want the cites to

the cases I talked about that likelihood is synonymous

with probability, I can give it to you.

CHAIRWOMAN RAMIREZ: Please.

MR. LECHNER: In re Terazosin Hydrochloride

Antitrust Litigation, 352 F.2d 1279, the word

"likelihood" is synonymous with "probability," citing

Shatel Corporation versus Mao Ta Lumber & Yacht,


Again, in defining the word "probability," the

Eleventh Circuit has recognized that it is capable of

two definitions, a lower "reasonable probability"

standard or a higher "more likely than not" standard.
But ultimately, the definition that is most often cited in the Eleventh Circuit precedent is the "more likely than not" standard. And that goes back to Terazosin and cites the Mercantile Tex. Corporation, 638 F.2d 1255, Fifth Circuit, 1981; U.S. v. Marine Bancorp, 418 U.S. 602 (1974). That deals with the Clayton Act. And it talks about there that it deals in probabilities, not ephemeral probabilities (sic), quoting Brown Shoe, 370 U.S. 292 at 1962.

In either incident, the trial counsel -- complaint counsel -- excuse me -- in this case has not carried the burden.

COMMISSIONER McSWEENY: Just let me clarify. The cases you were just citing are tort cases, a Clayton Act case --

MR. LECHNER: I'm sorry?

COMMISSIONER McSWEENY: These are tort cases --

MR. LECHNER: Well, one is a tort case, the other are commercial cases, so I've tried to cover both, yes. One is antitrust, and the other are tort cases, to my understanding, yes, so...

And I realize this is not a tort as we use that word in medical malpractice or architectural malpractice, but the concept is the same. There's an established standard, a deviation, both of which have to
be established on a basic -- on reasonable probability. An expert cannot testify to speculation. And then there has to be an opinion that because of that deviation, an injury or damage occurred, none of which have happened in this case.

Again, I go back to the fact that Dr. Hill only testified with regard to her conclusion. She started virtually every answer "It is my conclusion that." That's simply not appropriate testimony, and I respectfully suggest that it can't be considered as in any way proof in this case.

If I could just have one second.

CHAIRWOMAN RAMIREZ: Sure.

(Pause in the proceedings.)

COMMISSIONER OHLHAUSEN: Counsel, I have one more question.

MR. LECHNER: I'm sorry?

COMMISSIONER OHLHAUSEN: I have another question.

MR. LECHNER: Sure.

COMMISSIONER OHLHAUSEN: So if complaint counsel were to prove that or allege that the exposure of medical information to an unauthorized third party was substantial injury, so if they were to say that the fact that LabMD's data security practices exposed the
718 File to an unauthorized third party, which I think is shown in the record, why isn't that substantial injury?

MR. LECHNER: Well, if you look at all the circumstances, it was exposed to Tiversa, which is not a -- I assume, and there's nothing in the record to suggest that it is, that it is an identity theft user of these files.

Now, for argument sake, if we want to speculate that suppose there was proof that --

COMMISSIONER OHLHAUSEN: But let's say, for example, even if it wasn't for identity theft, they had the information about people's private medical medical diagnoses. Is that not an injury in itself?

MR. LECHNER: I don't see how it is. I see that it's a soft injury. It's not a substantial injury. It's not a concrete harm.

And the Commission through its counsel has been arguing that the standard they want to look at now is that it's likely that it raises the risk of concrete harm. Concrete harm is not, gee, I feel bad because somebody has looked at one of my documents. And I don't mean to sound callous on that.

But to go back to what you had asked before,
Commissioner, if there were proof that there were a
series of identity thieves that through their sites had
downloaded this, I think it might be a little bit more
easy with appropriate expert testimony to establish
that, but there is nothing here to suggest that.

Frankly, there's nothing here to suggest that
anyone read these documents other than the FTC and its
experts and perhaps that professor to whom Tiversa gave
it.

So to suggest this is really rank speculation on
rank speculation. Based on the facts of this case is
what we're constrained to look at right now.

If there's nothing further, I thank you for your
time.

CHAIRWOMAN RAMIREZ: Thank you, Counsel.

Ms. VanDruff, you used up all of your time, but
I know that you had reserved time for rebuttal, so --

MS. VANDRUFF: How would you like me to proceed,
Madam Chairwoman?

CHAIRWOMAN RAMIREZ: Why don't you go ahead.

MS. VANDRUFF: Okay. Thank you.

Respondent's counsel raised a number of issues
that I'd like to address in, unfortunately, no
particular order, if it pleases the Commission.

At the outset, respondent's counsel identified
Eagle Vision as something that was of particular interest because it was sophisticated technology. And I would just observe that that is something that is not in the record except through the testimony of Mr. Boback, a witness that the Administrative Law Judge found not to be credible and a witness upon whom complaint counsel is not relying.

And in fact, his testimony was contradicted by respondent's witness, Mr. Wallace, and that testimony can be found at complaint counsel's finding of fact 1394. It was Mr. Wallace's testimony that he found the 1718 File using a stand-alone computer and ordinary P2P software.

And you'll forgive me that -- one of you on the panel -- and I -- forgive me for not remembering which -- asked what happened to the computer, and it was respondent's counsel's response that it was speculation. But that's belied by the testimony. And in response to the question, I would direct the panel to complaint counsel's finding of fact 1409, which relates to the testimony of Mr. Daugherty, which describes a forensic examination performed by LabMD and what happened there.

LabMD is effectively out of business. That is in fact true. But I think it's important for a variety
of reasons, including the relief that complaint counsel is seeking, to note for the record that it intends to resume operations -- it made that point clear in the proceeding below -- and more importantly that when it resumes operations, it intends to apply the same protections to the data that it maintains for the 750,000 consumers. That is found at complaint counsel's finding of fact 61.

And that relates also to the question of what protections it has provided to data since 2010, a question that came up repeatedly during respondent counsel's presentation. And the weight of the evidence demonstrates that LabMD's unlawful conduct again continued after July of 2010.

I would direct the panel's consideration to complaint counsel's responses to respondent's findings of fact at paragraphs -- excuse me -- at findings 10(a) and 11 but just as examples.

As recently as November of 2013, paper records were stored in an unlocked, open garage at a personal residence. Key personnel were using weak user credentials, and critical vulnerabilities remained on key servers after vulnerability scans were completed.

Professor Hill's opinions don't support a contrary conclusion.
CHAIRWOMAN RAMIREZ: So, Counsel, let me interrupt you and just get to some -- again go back to some of the issues we already discussed with you but to hone in on certain of the positions articulated by respondent.

Respondent, as you know, argues that there really is no benchmark here, that Dr. Hill did not establish an appropriate measure by which to determine that the practices were reasonable or unreasonable, so what in the record should we be looking to in addition to -- you dispute that about Dr. Hill I know, but what else should we be looking to in the record to determine what the appropriate standard to apply here to determine reasonableness of LabMD's data security practices?

MS. VANDRUFF: Well, again, the legal standard, of course, is Section 5(n).

CHAIRWOMAN RAMIREZ: So I understand that.

MS. VANDRUFF: So with respect to that information security standard, in her expert report, she cites to a number of things, including a NIST guidance that goes back to 2002, which certainly predates any of the conduct that's challenged in this case.

CHAIRWOMAN RAMIREZ: So I understand that.
MS. VANDRUFF: Yes.

CHAIRWOMAN RAMIREZ: What else?

MS. VANDRUFF: Yes.

I'm not sure what else is cited in her report standing here, but I do believe that in her testimony and in her report she cites to other materials that were widely available and understood in the information security --

CHAIRWOMAN RAMIREZ: So another argument that respondent makes is that one needs to factor in the size of the operations of respondent, and is there any information about the cost of the reasonable security measures that you contend should have been utilized by LabMD?

MS. VANDRUFF: There is, yes. And Professor Hill, her opinions and her testimony addresses that. And all of the measures that she recommends to safeguard the information that was at risk of unauthorized disclosure were either at low or no cost for LabMD to implement and would require low-cost measures or staff time to have implemented.

So, for example, the failure of LabMD to have locked down computers, to have prevented employees from downloading software from the Internet, all that would have required was limiting administrative access.
That's something that is available -- that the IT staff could have done using a function through Windows, and it just would have required staff time to have enabled that function through Windows.

CHAIRWOMAN RAMIREZ: A couple more questions for you.

MS. VANDRUFF: Yes, Madam Chairwoman.

CHAIRWOMAN RAMIREZ: Respondent also argues that there is no evidence in the record that addresses the other elements of the unfairness standard aside from the question of injury, so can you tell me what is in the record on reasonable avoidance as well as countervailing benefits?

MS. VANDRUFF: Yes. I would be happy to address that.

The record establishes that consumers could not have reasonably avoided the significant risk of concrete harm that we have described at length this afternoon. In most cases, consumers had no way of knowing that LabMD would receive their personal information, much less any way of knowing --

CHAIRWOMAN RAMIREZ: And where do I look for this? Is this also in --

MS. VANDRUFF: Yes. The testimony of the physician practices. I regret that I cannot cite them to
you, but my colleague can (indicating).

    No. This is the low-cost measures. Excuse me.

The testimony of the physician practices

demonstrates that consumers did not know that their
information was going to LabMD, that that was a
decision made by their physicians. And moreover,
consumers had no reason to know of the data security
practices that LabMD undertook because they didn't even
know that their data was going to LabMD.

And as suggested by your earlier question, the
fact that LabMD's data security failures could have been
remedied at little or no cost, their failures,
therefore, did not provide any countervailing benefits to
consumers or competition; therefore, the remaining
prongs of Section 5(n) are met.

CHAIRWOMAN RAMIREZ: One final question at my
end that relates to the Sacramento documents.

    So respondent -- counsel for respondent argues
that we are limited to the allegations that are set
forth in the complaint. In particular, I believe it's
paragraph 10 that outlines data security practices with
regards to LabMD's computer network.

    Tell me why counsel for respondent is incorrect
in that regard, that we're not limited to the
allegations in the complaint.
MS. VANDRUFF: Well, the allegations in paragraph 10, again, are among other things. They are examples of failures of reasonable security, and so I think that the unfairness count is the gravamen of the --

CHAIRWOMAN RAMIREZ: Are there allegations in the complaint that relate more broadly to physical security in the complaint?

MS. VANDRUFF: No. But the allegations in paragraph 10 are consistent with allegations of physical security.

One point, before I move on from Sacramento, Madam Chairwoman, the respondent's counsel did say that it would be speculation about whether or not the Sacramento documents were from LabMD. Just as a matter of clarification, respondent's counsel earlier in the litigation, before respondent -- before Mr. Lechner joined the case, did stipulate that those documents were in fact LabMD's documents, just as a matter of clarification.

COMMISSIONER OHLHAUSEN: Counsel, I have a question.

MS. VANDRUFF: Yes.

COMMISSIONER OHLHAUSEN: So in the unfairness statement, mostly it talks about financial
injury, but it also says, "In an extreme case, however, where tangible injury could clearly be demonstrated, emotional effects might possibly be considered as the basis for a finding of unfairness."

So what evidence is in the record that the exposure of medical information about perhaps a stigmatizing condition to an unauthorized third party is substantial injury that it might cause this kind of tangible injury?

MS. VANDRUFF: May I have permission to respond to Commissioner Ohlhausen's question?

CHAIRWOMAN RAMIREZ: Please.

MS. VANDRUFF: The testimony of Mr. Kam addresses that question. He is an expert witness with experience specifically in medical identity theft and the harms that result from exposure of sensitive medical information. And his report and his testimony go to that question, and he describes the harms that result from the exposure of sensitive medical information and talks about exactly those kinds of harms.

COMMISSIONER OHLHAUSEN: Okay. Thank you.

MS. VANDRUFF: You're welcome.

CHAIRWOMAN RAMIREZ: Is it necessary for there to be actual harm for the information -- the medical
information that's exposed -- to be something that would be
potentially something that could stigmatize an
individual?

So let's just say the exposure has to do with
just routine blood tests. In your mind, would that
constitute actual harm?

Or is that a question that we don't need to
address?

MS. VANDRUFF: Well, it's a question that we
don't need to address in this case. That is certain.

In the -- because in this case the information that was
disclosed included potentially stigmatizing
information.

In the GMR case, the Commission alleged that
the information that was disclosed, which included
narrative notes from -- from physicians, could be
misused to cause substantial injury such as identity
theft and unauthorized access by disclosing sensitive
private medical information. We think that this is on
all fours with GMR.

MR. LECHNER: May I? I'm sorry.

CHAIRWOMAN RAMIREZ: Counsel?

MR. LECHNER: May I have leave just to make one
or two points?

CHAIRWOMAN RAMIREZ: Well, this is really out of
order, but given that we gave so much time to
Ms. VanDruff, I'll go ahead and allow you to make --

MR. LECHNER: Just two brief points.

CHAIRWOMAN RAMIREZ: Sure.

MS. VANDRUFF: Thank you, Madam Chairwoman.

MR. LECHNER: One point is that, to my
understanding, we did not stipulate that the Sacramento
documents came from our computer. We did not.

And secondly and the last point is, the Kam
opinion is bad based upon its bad methodology.

Those are the only two points. Thank you.

CHAIRWOMAN RAMIREZ: Thank you, Counsel.

Thank you very much.

We are adjourned. Thank you.

(Whereupon, the foregoing oral argument was
concluded at 2:37 p.m.)
CERTIFICATION OF REPORTER

DOCKET/FILE NUMBER: 9357

CASE TITLE: LabMD, Inc.

HEARING DATE: March 8, 2016

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: MARCH 10, 2016

JOSETT F. WHALEN, RMR

CERTIFICATION OF PROOFREADER

I HEREBY CERTIFY that I proofread the transcript for accuracy in spelling, hyphenation, punctuation and format.

ELIZABETH M. FARRELL