In the Matter of:

LabMD, Inc.

May 21, 2014
Trial - Public ██████████████
Volume 2

Condensed Transcript with Word Index

210

```
 1              FEDERAL TRADE COMMISSION
 2                   I N D E X
 3              IN RE LABMD, INC.
 4              TRIAL VOLUME 2
 5            PUBLIC AND ████████████
 6               MAY 21, 2014
 7
 8   WITNESS:      DIRECT   CROSS   REDIRECT   RECROSS   VOIR
 9   HILL                    214      311        319
10                                    324
11   WILMER         331      352
12   KAM            377
13
14
15   EXHIBITS   FOR ID  IN EVID  IN CAMERA  STRICKEN/REJECTED
16   CX
17   (none)
18
19   RX
20   (none)
21
22   JX
23   (none)
24
25
```

211

```
 1              UNITED STATES OF AMERICA
                FEDERAL TRADE COMMISSION
 2
 3   In the Matter of                  )
                                       )
 4   LabMD, Inc., a corporation,       ) Docket No. 9357
                                       )
 5                   Respondent.  )
     -------------------------------------)
 6
 7              May 21, 2014
 8               9:37 a.m.
 9             TRIAL VOLUME 2
10            PUBLIC AND ████████████
11
12   BEFORE THE HONORABLE D. MICHAEL CHAPPELL
13         Chief Administrative Law Judge
14            Federal Trade Commission
15         600 Pennsylvania Avenue, N.W.
16              Washington, D.C.
17
18
19    Reported by:  Josett F. Whalen, Court Reporter
20
21
22
23
24
25
```

212

```
 1   APPEARANCES:
 2
 3   ON BEHALF OF THE FEDERAL TRADE COMMISSION:
 4        LAURA RIPOSO VANDRUFF, ESQ.
 5        ALAIN SHEER, ESQ.
 6        MARGARET LASSACK, ESQ.
 7        RYAN MEHM, ESQ.
 8        Federal Trade Commission
 9        Bureau of Consumer Protection
10        Division of Privacy and Identity Protection
11        600 Pennsylvania Avenue, N.W.
12        Washington, D.C.   20580
13        (202) 326-2999
14        lvandruff@ftc.gov
15
16   ON BEHALF OF THE RESPONDENT:
17        WILLIAM A. SHERMAN, II, ESQ.
18        REED D. RUBINSTEIN, ESQ.
19        Dinsmore & Shohl LLP
20        801 Pennsylvania Avenue, N.W.
21        Suite 610
22        Washington, D.C.   20004
23        (202) 372-9100
24        william.sherman@dinsmore.com
25
```

213

```
 1   APPEARANCES: (continued)
 2
 3   ON BEHALF OF THE RESPONDENT:
 4        KENT G. HUNTINGTON, ESQ.
 5        HALLEE MORGAN, ESQ.
 6        MICHAEL PEPSON, ESQ.
 7        Cause of Action
 8        1919 Pennsylvania Avenue, N.W.
 9        Suite 650
10        Washington, D.C.   20006
11        (202) 499-2426
12        kent.huntington@causeofaction.org
13
14
15
16
17
18
19
20
21
22
23
24
25
```

1 (Pages 210 to 213)

214

```
 1           P R O C E E D I N G S
 2                  - - - - -
 3        JUDGE CHAPPELL:  Back on the record Docket 9357.
 4    I think we're ready for cross-exam.
 5        MR. SHERMAN:  We are, Your Honor.
 6        JUDGE CHAPPELL:  All right.  Proceed when ready.
 7                  - - - - -
 8    Whereupon --
 9           RAQUEL HILL, Ph.D.
10    a witness, called for examination, having been
11    previously duly sworn, was examined and testified
12    further as follows:
13            CROSS-EXAMINATION
14        BY MR. SHERMAN:
15        Q.  Good morning, Professor Hill.
16        A.  Good morning.
17        Q.  Professor, you testified for quite a long time
18    yesterday, and I just want to kind of go back and ask
19    you some follow-up questions with regard to your
20    testimony.  All right?
21        A.  Okay.
22        Q.  Yesterday, Professor, you indicated that in
23    doing your analysis of LabMD's data security, you were
24    asked to assume that there was harm; is that correct?
25        A.  Yes.
```

215

```
 1        Q.  Were you asked to assume any specific type of
 2    harm?
 3        A.  No.
 4        Q.  Were you asked to assume that this harm was
 5    caused by a lack or an inadequacy of LabMD's data
 6    security?
 7        A.  I don't -- I don't recall.
 8        JUDGE CHAPPELL:  I have a question along that
 9    line.
10        MR. SHERMAN:  Yes, sir.
11        JUDGE CHAPPELL:  And I haven't seen the reports.
12    I don't see this stuff.  I know they're exhibits now,
13    but I don't have them before trial.
14        Does your report detail what you were asked to
15    assume?
16        THE WITNESS:  Yes.  There's a statement in my
17    report about the harm that I was asked to assume.
18        JUDGE CHAPPELL:  Okay.  Thank you.
19        THE WITNESS:  There's a specific statement.
20        BY MR. SHERMAN:
21        Q.  Professor Hill, do you know where that statement
22    is located in your report?
23        Do you have a copy of your report?
24        A.  I do have a copy of my report.
25        JUDGE CHAPPELL:  As a follow-up to my question,
```

216

```
 1    did you make any assumptions that are not detailed in
 2    your report?
 3        THE WITNESS:  No, sir.
 4        JUDGE CHAPPELL:  Thank you.
 5        MR. SHERMAN:  And just for the clarity of the
 6    record, Your Honor, Professor Hill is looking at
 7    Exhibit -- is it CX 740? -- CX 740.
 8        BY MR. SHERMAN:
 9        Q.  Professor Hill, do you agree that CX 740 is the
10    report that you issued in regard to this litigation?
11        A.  Yes.
12        (Pause in the proceedings.)
13        MR. SHERMAN:  Does anybody know how to turn this
14    thing on (indicating)?  Is this thing on?
15        JUDGE CHAPPELL:  We just happen to have the guy
16    here who knows how to fix it.
17        (Discussion off the record.)
18        BY MR. SHERMAN:
19        Q.  Professor Hill, are you on page 18 of your
20    report?
21        A.  Yes.
22        Q.  And if you would, on page 18, the last sentence
23    in paragraph 49, can you read that into the record,
24    please.
25        A.  Yes.
```

217

```
 1        "For purposes of this report, I have assumed
 2    that these types of information can be used to harm
 3    consumers, through identity theft, medical identity
 4    theft, and disclosing private information."
 5        Q.  Professor Hill, were you asked to assume that
 6    this type of harm had actually occurred?
 7        A.  I was asked to assume that this type of harm
 8    could occur if the information was exposed.
 9        Q.  But you were not asked to assume that this type
10    of harm actually had occurred; is that correct?
11        A.  That's correct.
12        JUDGE CHAPPELL:  Whoa, whoa, whoa.  Wait a
13    minute.  Sorry to interrupt.
14        If you assumed it could occur, does that not
15    mean you assumed it was likely?  Isn't that the same
16    thing?
17        THE WITNESS:  I'm sorry, sir.  I thought that he
18    had said that it had --
19        JUDGE CHAPPELL:  No, no, I'm not talking about
20    what he said.
21        THE WITNESS:  Oh, okay.
22        JUDGE CHAPPELL:  I'm reading plain English
23    here.
24        Do you need her to read my question back?
25        THE WITNESS:  Yes, sir.
```

2 (Pages 214 to 217)

218

1   (The record was read as follows:)
2   "QUESTION: If you assumed it could occur, does
3   that not mean you assumed it was likely? Isn't that the
4   same thing?"
5   THE WITNESS: Oh, that it was likely? Yes, sir.
6   JUDGE CHAPPELL: Thank you.
7   Go ahead.
8   BY MR. SHERMAN:
9   Q. So it's fair to say then that you have no
10 opinion with regard to the likelihood of harm because it
11 was assumed in your report; correct?
12   A. I have no opinion, yes.
13   Q. Professor Hill, were you -- well, were you asked
14 to assume that the 1718 File -- do you know what that
15 is?
16   A. Yes.
17   Q. Okay. You agree the 1718 File is the insurance
18 aging file from LabMD that's at the center of this case;
19 correct?
20   A. Can -- I agree that I understand what the
21 1718 File is.
22   Q. And you've seen the 1718 File; is that correct?
23   A. Yes.
24   Q. Okay. And so you know what I'm talking about
25 when I refer to the 1718 File; correct?

219

1   A. Yes.
2   Q. Were you asked to assume that the 1718 File
3   escaped LabMD's possession because of some data
4   insecurity -- I'm sorry -- because of some inadequate
5   data security by LabMD?
6   A. Can you repeat your question.
7   Q. Maybe.
8   A. Please.
9   JUDGE CHAPPELL: Maybe restate it?
10   BY MR. SHERMAN:
11   Q. Were you asked to assume that the 1718 File
12 escaped the possession of LabMD due to some inadequacy
13 in LabMD's data security?
14   A. I was not asked to make any assumptions about
15 the inadequacies of LabMD's data security.
16   Q. Did you, in your research and review of the
17 evidence of record, conclude that the 1718 File escaped
18 LabMD's possession due to some inadequacy in LabMD's
19 data security?
20   A. Yes.
21   Q. And did you determine then or do you have an
22 opinion as to how the 1718 File escaped LabMD's
23 possession?
24   A. I don't have an opinion about how, exactly how
25 it escaped LabMD's possession.

220

1   Q. But it's fair to say that even not knowing how
2   it escaped, you attribute that escape to some inadequacy
3   in LabMD's data security.
4   A. Yes.
5   Q. Do you know specifically what inadequacy in
6   LabMD's data security you attribute the escape to?
7   A. Yes.
8   Q. Can you explain that to us, please.
9   A. The inadequacy that I saw was allowing employees
10 the ability to download software on their individual
11 workstations.
12   Q. Any software in particular?
13   A. The LimeWire software or any unauthorized
14 software, software not needed to do the job that the
15 employee was assigned to do.
16   Q. But in your review, there is no definitive
17 evidence of the record that you've reviewed that shows
18 that the 1718 File escaped LabMD's possession due to the
19 downloading of some unauthorized program onto a
20 workstation at LabMD.
21   A. There's no definitive evidence of how that file
22 left LabMD's possession.
23   Q. Is there any definitive evidence about how the
24 day sheets -- and are you familiar with the day sheets?
25   A. Yes, I am.

221

1   Q. Is there any definitive evidence of how the day
2   sheets left LabMD's possession based on your review of
3   the record?
4   A. No.
5   Q. Professor Hill, during your testimony, you
6   reviewed reports from a company called ProviDyn. Do you
7   recall that?
8   A. Yes.
9   Q. And you also reviewed reports from a company
10 called APT. Do you recall that as well?
11   A. Yes.
12   Q. Let's talk about your review of the reports from
13 a company called APT.
14   I recall your testimony -- and you correct me if
15 I'm wrong or misstating it -- that you testified that
16 you reviewed some reports from APT that indicated that
17 they had to eradicate viruses on LabMD's computer
18 network; is that correct?
19   A. The reports that I reviewed stated that they
20 were trying to run antivirus software but were unable
21 to.
22   Q. And in your review of those reports, were you
23 able to determine, during the relevant period, whether
24 or not -- well, let me back up.
25   Do you agree that the relevant time period for

3 (Pages 218 to 221)

222

1 your opinion is January 2005 through July of 2010?
2   A. Yes.
3   Q. Is it an accurate -- well, based on your review
4 of the record, are you able to determine whether or not
5 LabMD experienced any viruses on its network during the
6 relevant period?
7   A. Yes.
8   Q. And what determination did you make?
9   A. Regarding?
10   Q. As to whether or not LabMD experienced any
11 viruses on its network during the relevant period.
12   A. That they did.
13   Q. Okay. Do you know how many?
14   A. There -- I don't know exactly how many.
15   I recall there being one machine that had over a
16 thousand viruses on that particular machine.
17   There were servers that had multiple viruses
18 during the daily scans that were performed and the same
19 viruses were present for those consecutive days, which
20 indicates to me that those viruses were not removed
21 effectively.
22   Q. Is it abnormal for a company to have viruses on
23 their computers or on their computer network?
24   A. It's not abnormal for viruses to be found on
25 computers. It's a little bit abnormal for viruses to be

223

1 found on servers, because a server is not a machine
2 where you have an individual working on that machine.
3   When you have a human and they're doing
4 different things and interacting with various
5 applications and on the Internet, they may
6 inadvertently introduce viruses to the machine. But a
7 server is not a machine that you expect an individual
8 to be working on that machine and introducing those
9 types of risks.
10   Q. You said it's a little bit unusual, so in other
11 words, it happens, it occurs, doesn't it?
12   A. It is possible that it could occur.
13   Q. And it occurs in the normal course of business
14 for businesses that use computers and servers that
15 interact with the Internet; is that correct?
16   A. Yes, it does.
17   Q. And those viruses are eradicated by those
18 people who eradicate viruses; is that correct? Either
19 some IT staff in-house or some third-party service
20 provider comes in and they eradicate the virus;
21 correct?
22   A. There may be attempts to address the viruses.
23 The concern that I have is that there was no indication
24 that the viruses on the servers were eradicated because
25 you saw the exact same virus the following day.

224

1   Q. Is it your testimony that the viruses on the
2 servers of LabMD were not eradicated?
3   A. They didn't seem to be during that time period
4 that there were daily scans being performed, because
5 during the consecutive days you saw the exact same virus
6 and the exact same antispyware on the same machines,
7 so --
8   Q. Is it your testimony that they were never
9 eradicated?
10   A. No, that is not my testimony. I don't have
11 evidence regarding that they were never eradicated,
12 just during the time period that I -- for those daily
13 scans --
14   Q. And what is --
15   A. -- they were reoccurring.
16   Q. And what is that time period?
17   A. I don't recall the exact dates, but it was
18 within the relevant time period that those daily scans
19 were being performed. And I think -- but we would have
20 to go to that part of the record -- those scans were
21 being performed I think in 2010 for a series of maybe
22 over a month or maybe even longer. I don't recall the
23 exact dates, but I think it was in 2010.
24   Q. Okay. And so at some point after you saw the
25 occurrence of this virus for maybe a period of a month,

225

1 it was eradicated; is that correct?
2   A. I'm not sure. I can't make a statement about
3 that. I didn't -- I don't -- there wasn't evidence to
4 say that they were eradicated.
5   Q. Isn't it true that based on your review of the
6 record, that when these viruses would occur, there would
7 usually be a slowdown in LabMD's ability to work, a
8 slowdown in their ability to do what they do on a daily
9 basis?
10   A. In my review of the record, the IT staff were
11 called to fix a computer when there was a slowdown. One
12 virus may not cause a slowdown.
13   Q. Right.
14   And viruses cause different things to occur on
15 computers; is that correct?
16   A. Yes.
17   Q. Okay. And just because you have a virus on your
18 computer does not mean that the computer is inoperable,
19 does it?
20   A. Just because you have one, yes, it doesn't mean
21 that it's inoperable.
22   Q. Different viruses do different things; is that
23 correct?
24   A. Yes.
25   Q. And just because you have a certain virus on

4 (Pages 222 to 225)

226

1   your computer doesn't mean that your computer is exposed
2   to malicious outside intrusion other than that virus; is
3   that correct?
4   A. If there is any unauthorized software on your
5   machine, you can be susceptible to malicious outside
6   intrusion.
7   Q. Okay. And you can be susceptible to malicious
8   outside intrusion, but that does not necessarily occur;
9   is that correct?
10   A. It may not occur.
11   Q. It may not occur.
12   Are you aware of whether or not as a result of
13 any virus LabMD was susceptible to any -- I'm sorry.
14   Are you aware, as a result of any virus, whether
15 or not LabMD had a data security breach as a result of
16 that virus?
17   A. There was no evidence in the record to state
18 that.
19   Q. Let's talk about the ProviDyn report.
20   You reviewed the ProviDyn report in formulating
21 your opinion as well; is that correct?
22   A. Yes.
23   Q. And there were certain high-risk indications
24 that occurred as a result of the ProviDyn report, you
25 agree?

227

1   A. Yes.
2   Q. And in your review of the record, did LabMD
3   address those high-risk issues?
4   A. There was at least one that they did not
5   address.
6   Q. And which one was that?
7   A. That was the anonymous FTP risk.
8   Q. And the risk of the anonymous FTP was what?
9   A. The risk was that given anonymous FTP, you
10 didn't require an external entity to authenticate
11 itself, to prove its identity, so that exposed your
12 network to any external entity, and they could write and
13 have and take control over your machine. They could
14 read the data. They could turn your machine into a
15 data-serving machine and send that data anywhere.
16   Q. In your review of the record, was there any
17 evidence that that occurred?
18   A. There was no -- I didn't review any evidence.
19   Q. So there was no evidence, in your review of the
20 record, that someone was able to come in onto LabMD's
21 network and write, as you've described it, and then send
22 LabMD's information all over the Internet; is that
23 correct?
24   A. Yes. Because I -- that's correct because there
25 were no logs of the traffic that flowed into LabMD's

228

1   network and out of LabMD's network, so there were no
2   such logs in the record and I couldn't make such a
3   determination.
4   JUDGE CHAPPELL: I have a question.
5   THE WITNESS: Yes, sir.
6   JUDGE CHAPPELL: Are you aware of whether or not
7   any time a computer was on at LabMD it was on the
8   Internet, or did they have to click, for example, the
9   browser to be on the Internet?
10   THE WITNESS: If your computer is connected to
11 the Internet, it is accessible, you know, to the
12 Internet, so you don't necessarily have to click the
13 browser to be on the Internet. You're already connected
14 to the local area network, which is then connected to
15 the Internet via a router.
16   JUDGE CHAPPELL: So you're saying, based on
17 their local area network, if the computer was on, it
18 would have been on the Internet.
19   THE WITNESS: Yes, sir.
20   JUDGE CHAPPELL: That's not true on your home
21 computer, is it?
22   THE WITNESS: With your home computer, you are
23 connected to your ISP. And if someone knows your IP
24 address, you're already on the network if you're
25 connected to your home network, yes.

229

1   JUDGE CHAPPELL: So that would only be if your
2   router is turned on at home.
3   THE WITNESS: Only -- yes, sir.
4   JUDGE CHAPPELL: But at LabMD or any company
5   where you're on a LAN, if they have Internet access,
6   then someone -- that computer is always online whether
7   they know it or not.
8   THE WITNESS: Yes, sir.
9   JUDGE CHAPPELL: Effectively online.
10   THE WITNESS: Yes, sir.
11   JUDGE CHAPPELL: Thank you.
12   BY MR. SHERMAN:
13   Q. There were other high-risk indications from the
14 ProviDyn report; is that correct?
15   A. Yes, sir.
16   Q. Do you recall whether or not those risks were
17 addressed by LabMD?
18   A. I don't recall that they were not. I didn't
19 see any specific statements that they were not
20 addressed.
21   Q. Dr. Hill, you indicated in your testimony that
22 these high risks defined vulnerabilities to LabMD's
23 network; correct?
24   A. Yes.
25   Q. And in your testimony, you described all of the

230

1   negative impact or consequences of these
2   vulnerabilities; is that correct?
3   A. I specified some.
4   Q. You specified some but not all.
5   A. Not all.
6   Q. Is there any evidence in your review of the
7   record that any of these consequences that you specified
8   occurred at LabMD?
9   A. There's no evidence to support that, and as I've
10   previously stated, there were no such data logs that
11   will allow me to make such a conclusion.
12   Q. Dr. Hill, yesterday you also testified that in
13   arriving at your conclusions, you looked at standards in
14   the industry to determine whether or not LabMD's data
15   security met those standards; is that a fair statement
16   with regard to your testimony?
17   A. I think a more accurate statement would be, is
18   that I based my opinions on my knowledge within the area
19   and I supported my conclusions with the standards and
20   guidelines that I used.
21   Q. And you indicated that you looked at government
22   standards and guidelines; is that correct?
23   A. Yes.
24   Q. And did you look at FTC standards and guidelines
25   for data security?

231

1   A. I did not consider the FTC standards and
2   guidelines.
3   Q. Did you look at HIPAA -- and do you know what
4   HIPAA is?
5   A. Yes, sir, I do.
6   Q. Okay. And would you agree that HIPAA is a
7   regulation that governs the -- in part, governs the
8   storage and transfer of health-related information by
9   medical care providers?
10   A. I can't make a statement or -- about the legal
11   aspects of HIPAA and what it governs. I don't
12   understand the legal aspects of what it governs.
13   Q. So you're not intimately familiar with HIPAA
14   then.
15   A. No, sir.
16   Q. Okay. And you did not consider HIPAA or HIPAA's
17   guidelines in the formulation of your opinion in this
18   case; correct?
19   A. I considered the HIPAA security rule portion.
20   Q. And that's all with regard to HIPAA?
21   A. Yes.
22   Q. And so it didn't play into your consideration or
23   your opinion as to whether or not LabMD was a
24   HIPAA-covered entity.
25   A. No. I didn't take that into consideration.

232

1   Q. Can we pull up Appendix B to the report of
2   Ms. Hill, please.
3   A. Excuse me, Mr. Sherman.
4   Q. Yes.
5   A. There was also -- there were, as part of the
6   HIPAA documents, the six basic rules for risk
7   assessment, and that was also a HIPAA document that I
8   used.
9   Q. Professor Hill, you indicated that you
10   considered government standards in formulating your
11   opinion; is that correct?
12   A. Yes.
13   Q. And I believe one of the government standards
14   that you considered was NIST? And I won't ask you what
15   that stands for since I think we established that
16   yesterday through much wrangling.
17   But you did consider NIST; is that correct?
18   A. Yes. The 800-30 document from NIST.
19   Q. Was there any specific portion of NIST that you
20   considered to be relevant to LabMD's data security?
21   A. That particular document talks about risk
22   assessment practices, and yes, I considered that.
23   Q. How big is the NIST document that you
24   considered?
25   A. I don't recall that.

233

1   Q. Is it voluminous?
2   A. Voluminous?
3   Q. Yes.
4   Does it contain hundreds of pages?
5   A. No. I don't recall that it contains hundreds of
6   pages, no.
7   Q. And so in looking at NIST, you looked at it as
8   part of an overview and not in depth; would that be a
9   fair statement?
10   A. Yes. I was just looking at the specific
11   guidelines that they provided to support the conclusions
12   that I'd already made.
13   Q. And is it fair to say that you did the same for
14   all of the other government standards that are listed in
15   Appendix B to your report, that you looked at them as an
16   overview to support what you already knew? Is that
17   correct?
18   A. Yes. I was trying to find documents that
19   provided guidelines for security, and those documents
20   align with the recommendations that I made for a
21   comprehensive information security plan that was
22   reasonable and appropriate. Yes.
23   Q. So is it fair to say that the process you used
24   for coming up with your conclusion began with a review
25   of the evidence in the record in this case? Is that

6 (Pages 230 to 233)

234

1   correct?
2   A. Yes.
3   Q. Based on that review and based on your
4   knowledge, you then came to your conclusion with regard
5   to LabMD's data security; is that correct?
6   A. Yes.
7   Q. And then you went out in search of standards and
8   guidelines to support what you already knew.
9   A. I found documents. And I don't think it was a,
10   you know, big search for documents. These are
11   documents that IT professionals use for guidance, and
12   so...
13   Q. You testified yesterday that these were
14   standards and guidelines in the industry; correct?
15   A. What do you mean by "in the industry"?
16   Q. That was my next question to you.
17   When you testified that these are industry
18   standards, what industry were you talking about?
19   A. With regards to industry and government
20   standards, the industries relating to computer security
21   and information technology professionals. That's the
22   industry.
23   Q. So you were not referring to, in your
24   testimony, industry standards for medical care
25   providers.

235

1   A. There's a specific document that I cite from
2   the National Research Council that does provide
3   guidelines for protecting medical data, and those
4   guidelines are consistent with protection mechanisms
5   that are recommended by the other standards, so they're
6   consistent.
7   When you want to protect infrastructure, there
8   are some common guidelines that are across all types of
9   domains. Computing is pervasive, so these guidelines,
10   whether they're from NIST or from the Computer Emergency
11   Response Team or from the National Research Council that
12   specifically focused on medical data, they have
13   consistent guidelines. And that's because computing is
14   pervasive and consistent across different types of
15   business domains.
16   Q. And so you considered all of these sources to
17   the exclusion of HIPAA and to the exclusion of anything
18   out there that was available discussing data security
19   standards from the FTC; is that correct?
20   A. I don't quite understand your question. Can you
21   restate it.
22   Q. It's just that I want to make sure I'm getting
23   your testimony correct, that in reviewing standards and
24   guidelines for data security to assist in the
25   formulation or to support the formulation of your

236

1   opinion, you didn't consider the guidelines set out by
2   HIPAA, other than the security rule and the six
3   principles of risk assessment, and you didn't consider
4   any information that was out there with regard to
5   standards for data security from the FTC.
6   A. Yes, that is correct.
7   Q. Professor Hill, did you review the complaint in
8   this case prior to formulating your opinion?
9   A. Yes.
10   Q. And so are you familiar with the allegations in
11   paragraph 10 of the complaint?
12   And we can put them on the screen for you.
13   Would that help?
14   A. Yes. But let me back up. I think I misstated.
15   I began reviewing the documents before I ever
16   saw this complaint, and so I didn't formulate my
17   opinions after seeing the complaint, so I misstated. I
18   apologize.
19   Q. When did you start reviewing the documents in
20   this case, approximately?
21   A. I started reviewing the documents -- it was
22   either June or July of 2013. And I -- I'm thinking more
23   it's July, and I think I made that statement in the --
24   during the deposition, but I think it's July.
25   Q. And how long after you began reviewing the

237

1   documents did you see the complaint for the first time?
2   A. I think that I saw the complaint much later. I
3   recall seeing the complaint as I was preparing my expert
4   document, so that's when I recall seeing it.
5   Q. And so if you look at -- can you see the screen?
6   A. Yes, I can.
7   Q. If you look at paragraph 10 subparagraph (a).
8   A. Yes.
9   Q. It reads "did not develop, implement or maintain
10   a comprehensive information security program to protect
11   consumers' personal information."
12   Did I read that correct?
13   A. Yes.
14   Q. Now, you use that phrase "comprehensive
15   information security program" in your report; correct?
16   A. Yes.
17   Q. Who coined that phrase? Was that you or did you
18   look at the complaint and put that in your report?
19   A. I think we've discussed this before, but the --
20   that phrase is in some form of the concept of a
21   comprehensive information security program is
22   well-known, and that -- so the concept is known. The
23   exact phrase, as I've stated previously, I don't recall
24   if -- if, you know, I stated it or they stated it.
25   But I was asked to assess LabMD's security

7 (Pages 234 to 237)

238

1 program, and I may have been given the term
2 "comprehensive information security program." But that
3 whole concept of a comprehensive information security
4 program, that concept I know, so -- and that's why my
5 memory was vague on that, like whether they gave it to
6 me or not. But the notion of a -- when I was asked to
7 do, to assess their program, their security program,
8 that concept was there of a comprehensive information
9 security program.
10   JUDGE CHAPPELL: You said "we've discussed this
11 before." Who's "we"?
12   THE WITNESS: During the deposition. I'm sorry,
13 Your Honor.
14   BY MR. SHERMAN:
15   Q. It's a line of questioning that I asked you
16 during it; correct?
17   A. Yes.
18   Q. So your testimony is the concept of a
19 comprehensive information security program is out there
20 and known in the IT industry; correct?
21   A. Yes.
22   Q. What about the phrase "comprehensive information
23 security program"?
24   A. I would -- I would say that "comprehensive
25 information security program," whether that phrase is

239

1 there or that's how it is expressed -- and it may be
2 that terminology may be used and in some circles and it
3 may not be, but that whole idea of a comprehensive
4 information security program is there.
5   Q. Do you find that phrase, not the concept, that
6 phrase, used in the literature that you reviewed to
7 support your opinion here?
8   A. I don't recall.
9   Q. Now, you define a comprehensive security program
10 in your report.
11   If we can go to the report on page 19. We may
12 continue to switch back and forth between those two
13 documents, please.
14   Do you have your report in front of you,
15 Professor Hill?
16   A. Yes, I do.
17   Q. Could you turn to page 19, please.
18   Professor Hill, I direct your attention to
19 paragraph 52 of your report.
20   A. Yes.
21   Q. Would you agree that that is your definition of
22 what a comprehensive information security program is?
23   A. I would say that that is not only my definition
24 of what a comprehensive information security program is,
25 but it is an accepted definition throughout the IT

240

1 profession.
2   Q. Could you read that definition into the record
3 for us, please.
4   A. "A comprehensive information security program is
5 a plan that sets out an organization's security goals,
6 the written policies that would satisfy those goals, the
7 mechanisms that would be used to enforce the written
8 policies, and how those mechanisms would be used to
9 enforce the written policies. The best practices for
10 developing a comprehensive information security program
11 would include the seven principles that I discuss in
12 paragraph 31, above: don't keep what you don't need,
13 patch, ports, policies, protect, probe and physical."
14   Q. Professor Hill, could one find that definition
15 of "comprehensive information security program" out in
16 the literature that you searched to support your opinion
17 for this case?
18   A. I think that one could find all of the elements
19 that I've included in this definition. Yes.
20   Q. But not specifically that definition as you've
21 worded it.
22   A. Probably not specifically that phrasing.
23   Q. Do you know if the term and the definition of
24 "comprehensive information security program" is
25 contained within any of the data security literature

241

1 that has been published by the FTC?
2   A. I don't know. I didn't review the FTC's
3 document on security.
4   Q. Are you suggesting that there is a document from
5 the FTC on security?
6   A. I think that there is.
7   Q. And what do you think it is?
8   A. Excuse me?
9   Q. What do you think that document is?
10   A. I think that the FTC has a document that has
11 security recommendations. I didn't review it, but I do
12 recall seeing it.
13   Q. Do you know whether or not that document
14 contains the phrase and the definition of
15 "comprehensive information security program"?
16   A. No, I do not.
17   JUDGE CHAPPELL: Mr. Sherman, do you plan on
18 using that billboard, whatever that's called there,
19 during your cross?
20   MR. SHERMAN: I do.
21   JUDGE CHAPPELL: Okay.
22   BY MR. SHERMAN:
23   Q. Now, Professor Hill, you would agree then that
24 your report tracks the language in paragraph 10 of the
25 complaint in terms of delineating LabMD's data security

8 (Pages 238 to 241)

242

1 inadequacies.
2   A. Yes.
3   Q. And so is it fair to say then that your report
4 is based on the complaint or the complaint is based on
5 your report?
6   A. It is fair to say that I was asked to offer
7 opinions in those areas.
8   Q. Were those areas given to you as they appear in
9 the complaint?
10   A. Yes.
11   Q. Now, you indicate that there are seven
12 principles to developing a comprehensive information
13 security program; correct?
14   A. Yes.
15   Q. Those principles are: don't keep what you don't
16 need, patch, ports, policies, protect, probe, and
17 physical; correct?
18   A. Yes.
19   Q. In the research of the documents, the standards,
20 the guidelines that are out there, are these seven
21 principles, as you list them, anywhere else in one
22 document and incorporated as the seven principles of a
23 comprehensive information security program?
24   A. I don't recall the principles being stated in
25 that way, that these are the seven principles for a

243

1 comprehensive information security plan.
2   I do recall in those documents that you have at
3 least six of those principles present in some form. The
4 one that may not be present is the "don't keep what you
5 don't need." And it is my opinion that is because the
6 documents that I reference are documents that were
7 created prior or during the relevant time period, and
8 some of these documents are prior to the beginning of
9 the relevant time period.
10   The "don't keep what you don't need" principle
11 is more about data. And what we see emerging is a trend
12 where data is becoming a major part of organizations'
13 business model.
14   And so now that we are amassing more and more
15 data, there is the need to protect this data and limit
16 access to this data, and so that's why you may not see
17 and you probably wouldn't see it in those exact terms
18 of "don't keep what you don't need." You may see terms
19 "like limit access to data." But that need to limit
20 access is something that is emerging because we have
21 this emerging trend of large amounts of data and
22 organizations maintaining large amounts of data.
23   Q. So if I'm an IT professional and I'm looking
24 for the seven principles of a comprehensive information
25 security plan and program, am I going to be able to

244

1 find that somewhere where it says a comprehensive
2 information security program consists of these seven
3 principles?
4   A. What you would be able to find are documents
5 that give you recommendations that contain those
6 principles. Yes, you'll be able to find that. The
7 exact phrasing "a comprehensive information security
8 program consists of these seven principles," you may not
9 find that exact phrasing, but you will find
10 recommendations and guidelines that encompass those
11 seven principles.
12   Q. So if I'm doing this research, I'm likely to
13 have to look at a variety of documents to conclude then
14 that seven principles of a comprehensive information
15 security program, whose definition I have to glean also
16 from all of these documents, incorporates these seven
17 principles.
18   A. No. I don't -- I don't agree with that.
19 Because as I've previously stated, these guidelines,
20 whether they are for a specific domain or general
21 guidelines, they are consistent. They're basically
22 stating the same thing, that if you want to protect
23 your system, these are the set of things that you
24 have -- that you want to do. And they provide general
25 guidelines for protecting a system that are consistent.

245

1   So you can take a look at one of them and,
2 you know, find these specific principles embedded in
3 those recommendations, so I don't agree that you have to
4 look in multiple places to find these general
5 principles. Because these are -- these are general
6 principles that are used to protect computing
7 infrastructure. These are -- this is nothing special
8 here.
9   Q. So there's a document that contains all of these
10 terms and says, you know, basically this is what you
11 should be doing in order to develop a comprehensive
12 information security program.
13   A. As I've stated before, the terms may not be the
14 exact same, but the concepts of doing updates, patching,
15 closing unused ports, specifying strong password
16 policies, all of those concepts are captured in general
17 guidelines. These -- providing access control and
18 limiting access to your data, these are very basic
19 recommendations that anyone would use to protect their
20 infrastructure. There's nothing special about these.
21   And so those guidelines that, you know, for
22 small businesses that I've cited and other guidelines
23 for doing overall security, they capture those
24 principles in their recommendations.
25   Q. And so other than the one document that you

9 (Pages 242 to 245)

                                                                    246

1   named that specifically addressed healthcare entities,
2   are you aware of any other government standards for the
3   regulation of healthcare data?
4   A. For the regulation of healthcare data?
5   Q. For the regulation or that gives guidelines for
6   data security as it relates to healthcare.
7   A. I think that I've cited a couple of documents.
8   That was the security rule from HIPAA. There was the
9   six basic principles for risk assessment. There was the
10   one from the National Research Council about protecting
11   medical data.
12   I cited documents that were written prior to or
13   within -- early within the relevant time period. I
14   think that there are later documents that may say
15   something specifically about medical-related data, but I
16   didn't cite those because I wanted to cite documents
17   that were available within -- during the relevant time
18   period.
19   So there may be other documents, but I didn't --
20   I didn't cite those.
21   Q. But you would agree that the first two documents
22   you named are HIPAA documents.
23   A. The first two documents that I named are HIPAA
24   documents, but the National Research Council document is
25   not a HIPAA document.

                                                                    247

1   Q. Could you turn to page 24 of your report,
2   please.
3   Are you there?
4   A. Yes.
5   Q. In paragraph 63, you indicate that complaint
6   counsel asked you to provide an opinion as to whether
7   LabMD used readily available measures to identify
8   commonly known or reasonably foreseeable security risks
9   and vulnerabilities on its network, which is often
10   called "risk assessment" in the IT field.
11   Did I read that correctly?
12   A. Yes.
13   Q. And would you agree then -- can you go back to
14   the complaint -- that that corresponds with the
15   complaint, with subparagraph (b) of the complaint?
16   A. Yes.
17   Q. Okay. Now, in determining whether LabMD used
18   readily available measures to identify commonly known or
19   reasonably foreseeable security risks and
20   vulnerabilities on its networks, what did you look at
21   specifically?
22   A. I -- I looked at the lack of information
23   regarding risk assessment. There were no specific
24   policies on risk assessment.
25   And what I saw was that antivirus software was

                                                                    248

1   used to detect malware and that there were times when
2   the antivirus software was not functional.
3   I saw no evidence of firewall logs, but I saw
4   some evidence that they were being reviewed and those
5   reviews indicated that there were attempts to gain
6   unauthorized access to LabMD's network.
7   But outside of firewall logs, firewall logs and
8   antivirus software, I didn't see any other risk
9   assessments until 2010, when the penetration test and
10   vulnerability assessment was done by ProviDyn.
11   Q. So in terms of risk assessment, LabMD had in
12   place antivirus software; correct?
13   A. Yes.
14   Q. And in terms of risk assessment, LabMD had in
15   place firewalls that logged penetration attempts?
16   A. There was testimony that the logs were reviewed
17   and the person reviewing them saw that there were
18   attempts to penetrate the network.
19   Q. Okay.
20   A. So the firewall --
21   Q. So they had this in place, but it wasn't good
22   enough, in your opinion; correct?
23   A. They had it in place. It wasn't sufficient to
24   assess the risk within their system, as pointed out by
25   the penetration test and the vulnerability assessment

                                                                    249

1   that was done by ProviDyn, which identified
2   vulnerabilities that had been present in the network for
3   years.
4   Q. So you've indicated that the firewall logs
5   indicated penetration attempts, and the ProviDyn
6   penetration test indicated vulnerabilities; correct?
7   A. Yes.
8   Q. But what actually happened?
9   A. There are no logs to determine what actually
10   happened.
11   Q. But this -- these could have happened, they were
12   vulnerable to certain things that could have happened;
13   right?
14   A. They were vulnerable to things that could have
15   happened, and given the risk level, it was -- there was
16   a large probability that they -- those vulnerabilities
17   could be exploited. And that's why they were rated with
18   high risk.
19   Q. I've finally figured out a way to make this
20   easier for both of us.
21   Could you turn to page 16 of your report.
22   A. Okay.
23   Q. As we look at page 16 paragraph 45, you actually
24   restate paragraph 10 and its subparagraphs of the
25   complaint; correct?

                                              10 (Pages 246 to 249)

250

1   A. Yes.
2   Q. And so moving down to the third bullet point,
3   which is subparagraph (c) of the complaint, it reads
4   "did not use adequate measures to prevent employees from
5   accessing personal information not needed to perform
6   their jobs."
7   Do you see that?
8   A. Yes.
9   Q. And that was one of the things that you were
10   asked to determine, and your finding was what?
11   A. That they did not use adequate measures to
12   prevent employees from accessing personal information
13   not needed to do their jobs.
14   Q. Let me go back. I forgot to ask you a couple of
15   questions. I apologize.
16   A. Okay.
17   Q. In establishing a comprehensive information
18   security program, how important is it for that to be in
19   writing?
20   A. It's very important for it to be in writing.
21   Q. Why?
22   A. Because the -- having the policies and the
23   enforcement mechanisms that are to be used to enforce
24   those policies and your overall security guidelines in
25   writing, they provide a road map for the IT

251

1   professionals that are to -- that are responsible for
2   implementing that program. They also provide training
3   in a sense about the process that was used to create
4   that plan.
5   And it's also important to have it in writing
6   because there's -- turnover will occur, and this
7   provides the history of how the infrastructure was
8   protected, and so it provides guidance to those
9   individuals who will be employed in that position and be
10   responsible for maintaining that.
11   And another reason would be is that threats are
12   emerging. There are new threats every day. And you
13   need to understand what you're currently doing in order
14   to determine how you would need to evolve your current
15   plan to address the new vulnerabilities.
16   Q. So having it in writing provides awareness?
17   A. Yes.
18   Q. Not only of the IT professional but for the
19   employees; is that right?
20   A. Yes.
21   Q. And so being aware of the policy is important;
22   correct?
23   A. Being aware of the policy is important, and it's
24   beyond awareness because there needs to be documentation
25   for all of these, all of these reasons.

252

1   Q. So awareness through documentation.
2   A. Awareness through documentation and knowledge.
3   So just being aware that there is a policy may
4   not be sufficient to understand what the policy is, what
5   it's supposed to protect, and how you're going to
6   enforce the policy.
7   Q. It also assists, would you agree, in those who
8   would fall under the policy complying with that policy;
9   correct?
10   A. Yes.
11   MR. SHERMAN: If I could have a moment,
12   Your Honor. I'm sorry.
13   (Pause in the proceedings.)
14   BY MR. SHERMAN:
15   Q. So if we go back to page 16, subparagraph (c) of
16   paragraph 45, did not use adequate measures to prevent
17   employees from accessing personal information not needed
18   to perform their jobs; correct?
19   A. Yes.
20   Q. What did you review in order to make this
21   determination?
22   A. I reviewed evidence that -- that allowed me to
23   determine that LabMD maintained approximately a hundred
24   thousand records for individuals for which they never
25   provided a service to. That was one thing that I

253

1   reviewed. And also evidence that LabMD was unable to
2   determine exactly what types of information that their
3   employees needed in order to do their jobs, so without
4   that determination, you can't limit or restrict access.
5   Q. Did you review deposition testimony?
6   A. Yes, I did also.
7   Q. Okay. Simmons page 58.
8   Let's go to Hyer page 139.
9   I apologize, Your Honor.
10   (Pause in the proceedings.)
11   Professor Hill, do you recall reviewing the
12   deposition testimony of Mr. Christopher Maire?
13   A. Yes.
14   Q. And is it fair to say that Christopher Maire was
15   an IT employee at LabMD during the relevant period of
16   time?
17   A. Yes.
18   Q. And what I've pulled up is page 81 of
19   Mr. Maire's testimony.
20   MS. LASSACK: I want to clarify that exhibit
21   number showing that what's on the screen is what it
22   purports to be.
23   MR. SHERMAN: There's an exhibit number on
24   the --
25   MS. LASSACK: I'm unable to see on the screen,

11 (Pages 250 to 253)

254

1   Your Honor.
2   MR. SHERMAN: That's why I was going for the
3   exhibit number, because I can't see it either.
4   BY MR. SHERMAN:
5   **Q. Well, you do recall reviewing the testimony of**
6   **Christopher Maire; is that correct?**
7   A. Yes.
8   **Q. And up on the screen is page -- I'll represent**
9   **to you currently that up on the screen is page 81 of**
10 **that deposition testimony.**
11   **Can you read that testimony, please.**
12   **I'm sorry. You can see it from where you are;**
13 **is that correct?**
14   A. I can see it, yes.
15   **Q. Okay.**
16   A. If you could enlarge it just -- if it's
17 possible. If not, I -- thank you.
18   **Q. And I'm referring specifically to page -- I'm**
19 **sorry -- line 18, which says, "To your knowledge, did**
20 **LabMD employees have access to information that they did**
21 **not need to do their jobs?"**
22   **The witness said, "Not to my knowledge."**
23   **Correct?**
24   A. Yes, that's what it says.
25   **Q. Okay. And if we go on to page 108...**

255

1   **(Pause in the proceedings.)**
2   **Your Honor, could we take a break?**
3   JUDGE CHAPPELL: Okay. We're going to take a
4   break, but I expect you to get these -- I don't know
5   what we're calling these. I don't know if it's not
6   being prepared or not having things together, but I
7   expect this to be taken care of during the break.
8   MR. SHERMAN: I understand, Your Honor.
9   JUDGE CHAPPELL: Because I've been very lenient
10 letting this go on all morning off and on, so let's get
11 it together.
12   MR. SHERMAN: Yes, sir. Thank you, Your Honor.
13   JUDGE CHAPPELL: It will be a moment before we
14 take a break.
15   (Pause in the proceedings.)
16   We're going to reconvene at 11:20.
17   We're in recess.
18   (Recess)
19   JUDGE CHAPPELL: Back on the record.
20   MR. SHERMAN: Thank you, Your Honor.
21   JUDGE CHAPPELL: Just a note on the courtroom
22 environment. You might think it's chilly in here. For
23 one thing, it keeps people awake and frosty. The other
24 thing, when it's 90 degrees outside, it won't feel like
25 this in here. We just kind of leave it set the way it's

256

1   set. That's how we survive when it's really hot
2   outside.
3   I want to talk about some witness scheduling
4   before you get back into the questioning.
5   We talked yesterday about going late on Friday,
6   and I thought I heard that Mr. -- that the witness
7   Van Dyke was going to be Friday.
8   Has there been a change? Is it now going to be
9   someone named Shields?
10   MR. SHEER: Your Honor, it may be
11 Professor Clay Shields from the computer science
12 department at Georgetown University, but there also is
13 the Dean Johnson, who is available on Friday and is
14 going to be presented by the respondent.
15   JUDGE CHAPPELL: Right. That's the witness out
16 of order.
17   MR. SHERMAN: That's correct, Your Honor.
18   JUDGE CHAPPELL: But I --
19   MR. SHERMAN: It's also my understanding that
20 Mr. Shields is a rebuttal witness. I mean, he gave a
21 rebuttal report to our expert witness report. And I
22 don't pretend to know the procedure to that extent, but
23 it seems to me that he's being called somewhat
24 prematurely before our expert has an opportunity to
25 testify.

257

1   JUDGE CHAPPELL: So are you going to object to
2   them calling him before?
3   MR. SHERMAN: I would.
4   JUDGE CHAPPELL: All right. I would suggest
5   that you two work on that.
6   For your purposes as respondent, he has to keep
7   to what's in his report. As far as I'm concerned, I
8   don't care if he's here the first day or the last day.
9   But the rule in this court is, if you are an expert, you
10 have to have a report, and that report is it. You don't
11 go beyond that.
12   MR. SHERMAN: If that's the case, Your Honor, I
13 will withdraw any objection I would have to calling
14 Mr. Shields.
15   Do you intend to call him Friday?
16   MR. SHEER: We do.
17   JUDGE CHAPPELL: My concern was it was going to
18 be unrealistic to finish Mr. Johnson on Friday, because
19 even though we'll go late, I'm not going to require
20 everyone required to keep the court going beyond
21 7:00 p.m. That's the outside limit, is 7:00 p.m.
22   MR. SHERMAN: My examination of Mr. Johnson I do
23 not imagine will be longer than a couple of hours, if
24 that.
25   JUDGE CHAPPELL: All right. The only reason I

258

1   brought it up is, I want to have whoever you're
2   scheduling for Friday, I want him here in the event they
3   can start Thursday. And if we -- you know, if your
4   witness finishes at 4:30 Thursday, that next witness
5   needs to be here, so we can get started on it. That
6   way, we have some hope of finishing everything that we
7   plan to by Friday.
8   MR. SHEER: Understood, Your Honor.
9   MR. SHERMAN: So Van Dyke is not coming?
10   MR. SHEER: He is coming.
11   MR. SHERMAN: Is he coming Friday?
12   MR. SHEER: I don't think he's coming Friday. I
13   think he's coming -- we'll talk during the break.
14   JUDGE CHAPPELL: Do you need to have a
15   discussion again?
16   MR. SHERMAN: Not right now, Your Honor. I'm
17   sure we can do it on the break.
18   JUDGE CHAPPELL: The other thing I wanted to
19   mention is, regarding experts, I just want to make
20   clear what I expect.
21   When you call an expert witness -- this goes
22   for everyone -- feel free to go over the basics, where
23   they went to school, you know, their training, their --
24   what job they're doing, their educational background,
25   but unless it's relevant to the opinions, I really don't

259

1   need you going into, like I said yesterday, CVs,
2   dissertations, areas that are in the past. I'm
3   expecting that's in the record as a CV.
4   If you think you have a need to do that -- and
5   I'm telling you that while you still have a witness
6   here -- if you think you want to put that in the record,
7   go ahead. I don't see a need for it. Like I say, the
8   CV is in the record, so that should be covered.
9   But I expect you to call them, I expect you to
10   go into where they work now, where they have worked and
11   their educational background, and beyond that, I don't
12   really need to hear it. I believe that anything I need
13   to look at in the qualifications will be in a CV that
14   will be in the record as an exhibit.
15   But I'm not telling you exactly what to do or
16   not do. I'm just telling you what I expect.
17   Any questions on that?
18   MR. SHERMAN: No, sir.
19   MR. SHEER: No, Your Honor.
20   JUDGE CHAPPELL: All right. Thank you.
21   Go ahead.
22   BY MR. SHERMAN:
23   **Q. Professor Hill, we were discussing**
24   **page 16 subparagraph (c), did not use adequate measures**
25   **to prevent employees from accessing personal**

260

1   **information needed to perform their jobs, when we took a**
2   **break.**
3   **Are you there?**
4   A. One moment, please.
5   Yes.
6   **Q. And I believe it's your testimony -- I want to**
7   **clarify it before we go further -- that the reason why**
8   **you concluded that LabMD did not use adequate measures**
9   **to prevent employees from accessing personal information**
10   **not needed to perform their jobs was because, in**
11   **response to an interrogatory request that you reviewed,**
12   **LabMD was not able to specifically name for the relevant**
13   **period each employee and what access that employee had**
14   **to information on LabMD's network.**
15   A. I didn't specify each employee, but I think that
16   there are different types of employees at LabMD, and --
17   and LabMD was not able to specify the types of
18   information that those employees had access to. That
19   was one reason for my opinion.
20   And the second was that there was information
21   that LabMD maintained about individuals for which they
22   had never provided services for.
23   **Q. Okay. Did you review deposition testimony in**
24   **formulating your opinion on this particular issue?**
25   A. Yes.

261

1   **Q. And do you recall reviewing the testimony of one**
2   **Christopher Maire?**
3   A. Yes.
4   **Q. Okay. And on the screen I'll submit that this**
5   **is Exhibit CX 724, an excerpt of Christopher Maire's**
6   **testimony at page 106.**
7   **Do you see that on the screen?**
8   A. Yes, I do.
9   **Q. I would actually ask you to look at**
10   **page 108 down at the bottom, where it says:**
11   **"QUESTION: So is it fair and accurate to say**
12   **that Internet access for billing clerks at LabMD during**
13   **your tenure was limited to management-approved sites**
14   **from which they could gather information concerning**
15   **billing which would help them do their jobs?**
16   **"ANSWER: Yes."**
17   **Did I read that correctly?**
18   A. Yes, you did.
19   JUDGE CHAPPELL: May I suggest, so the record is
20   clear, could you have the witness identify who Mr. Maire
21   is, what his position was.
22   MR. SHERMAN: If she can recall, Your Honor.
23   BY MR. SHERMAN:
24   **Q. Do you recall whether or not Mr. Maire was an**
25   **IT employee at LabMD?**

13 (Pages 258 to 261)

262

1   A. Yes. He was an IT employee.
2   Q. And if you turn to page 109, at line 18 -- I'm
3   sorry -- line 16:
4   "QUESTION: And did the managers in the billing
5   department have access to the Internet?
6   "ANSWER: Yes.
7   "QUESTION: And that access was unlimited?
8   "ANSWER: Correct.
9   "QUESTION: Did the employees in the LabMD
10 billing department have access to information concerning
11 lab results?
12   "ANSWER: Particular results, I'm not sure.
13 However, they did have access to know what to bill for.
14   "QUESTION: I see.
15   "Was the information which they, meaning the
16 persons in the billing department, had access to with
17 regard to information, was that limited?
18   "ANSWER: Repeat the question. I'm sorry."
19   The question was repeated.
20   "QUESTION: In terms of the information that the
21 employees in the billing department had with regard to
22 information from the lab side of the business, was that
23 access limited?
24   "ANSWER: Yes.
25   "QUESTION: How was that access limited?

263

1   "ANSWER: They were not given permission to,
2   say, the actual lab results and that software. The
3   results should have -- should not have resided anywhere
4   else other than in the database and the laboratory
5   software where it resided."
6   Am I reading that correctly?
7   A. Yes.
8   Q. Did you consider this testimony when you
9   formulated your opinion with regard to whether certain
10 employees at LabMD had limited access in order to
11 perform their jobs?
12   A. I considered this testimony. And I also
13 considered other testimony from transcripts that also
14 stated that in addition to information from the billing
15 software that they also had access from information from
16 the overall database that contained lab-related
17 information.
18   So I considered this testimony and testimony
19 from other IT staff.
20   Q. Was it your understanding that the billing
21 department employees needed access to information from
22 the lab side of the business in order to complete their
23 billing functions and to determine what insurance
24 billing codes needed to be used for the tests that were
25 performed?

264

1   A. It is my understanding that they needed
2   information to do their job. Specifically what that
3   information is, I'm not -- I can't make a statement
4   about that.
5   But I feel that employees should have access to
6   whatever information that they need in order to do their
7   jobs, but the organization should be able to specify
8   what that information is.
9   And I apologize. My voice is -- is leaving a
10 little bit, so...
11   Q. Do you have water, coffee or something?
12   A. Yes. I have some hot water here.
13   Q. If you look on page 112 of the same exhibit,
14 line 5:
15   "QUESTION: So is it fair then to say that
16 employees in the billing department did not have access
17 to information from the sales department?
18   "ANSWER: I would say that's a fair
19 assumption."
20   You reviewed this testimony, and your general
21 overall opinion remained the same; is that correct?
22   A. Yes.
23   Q. Same page, line 19 -- I'm sorry. Page 6 -- I'm
24 sorry -- line 13:
25   "QUESTION: Was it also true that sales could

265

1   not access billing information?
2   "ANSWER: That is correct.
3   "QUESTION: Is it also true that persons
4   involved in sales could not access laboratory
5   information?
6   "ANSWER: That is correct.
7   "QUESTION: Is it also your understanding based
8   on your involvement at LabMD that persons employed in
9   the laboratory department did not have access to sales
10 information?
11   "ANSWER: Correct."
12   Did you review this testimony prior to coming to
13 your conclusion?
14   A. I reviewed this testimony. But there was no
15 evidence in the record of how the statements that are
16 made by Mr. Maire were actually enforced. There were no
17 specific access control policies that were stated.
18   Q. There were no specific access control policies
19 in writing; is that correct?
20   A. There were no specific access control policies
21 or specific statements about what those policies were.
22   Q. So despite Mr. Maire's understanding that it was
23 true that persons involved in sales could not access
24 laboratory information, because that information was not
25 in writing or there was no stated policy, you concluded

14 (Pages 262 to 265)

266

1   that that's not true?
2   A. I couldn't draw a conclusion about what
3   information employees had access to because there was
4   very specific statements that they had access to various
5   levels of information.
6   He's stating that billings people may have
7   access to some information, that salespeople have access
8   to others. It is my understanding that salespeople did
9   not have access to specific consumer personal
10   information. And from the record -- and that is stated
11   not only in Maire's testimony but in other testimony, so
12   I'm not concerned about salespeople. That didn't impact
13   my opinion about limiting access to personal
14   information. It is my understanding that they didn't
15   have access, the salespeople didn't.
16   Q. Okay. The same page, 112, down at the bottom:
17   "QUESTION: Is it also your understanding that
18   persons involved in the laboratory department did not
19   have access" -- and we go to the next page, 113 -- "to
20   information in the billing department?
21   "ANSWER: Correct."
22   So while the people in the sales department
23   didn't have access to personal information, correct, you
24   accepted that based on the testimony that you reviewed;
25   correct?

267

1   A. Yes.
2   Q. Did you accept the fact, based on the testimony
3   that you reviewed, that persons involved in the
4   laboratory department did not have access to information
5   in the billing department?
6   A. With regards to the people in the laboratory
7   department and what information that they had access to,
8   I think that there is testimony that there's some
9   overlap in the information that the two groups had
10   access to.
11   So I think that there would need to be some
12   overlap because the people in the laboratory would need
13   access to the individual, the test that needed to be
14   performed, and so would the billings people.
15   So I don't think that this testimony accurately
16   reflects that overlap because it says that people in the
17   laboratory department does not have access to
18   information that people in the billings department have
19   access to. I'm not sure that that's an accurate
20   statement.
21   Q. Well, let me put it this way. And I could take
22   your answer a couple of ways.
23   Are you saying that because the people in the
24   billing department had access to personal information
25   and the people in the laboratory department had access

268

1   to the same personal information that you found then
2   that the access was not limited?
3   A. No. That's not what I'm stating.
4   Q. Can I ask you another question before you
5   explain?
6   A. Yes.
7   Q. So it clearly states here that the people in the
8   laboratory department did not have access to information
9   in the billing department; correct?
10   A. Yes.
11   Q. And I'm trying to figure out what your
12   contention is that the access to information was not
13   adequately limited as it relates to those two
14   departments.
15   A. What my statement is regarding to limitation is
16   that within the record there is no specification of what
17   an employee -- the types of information that an employee
18   would need in order to perform his or her job. And
19   because that is not specified, then you will not be able
20   to limit access. That's what I am stating about the
21   inability of LabMD to restrict access.
22   Q. Is your testimony, the answer you just gave,
23   that there's nothing in the record that indicates that
24   limited access from the laboratory department to the
25   billing department information is not in writing, and

269

1   that's why you believe that there is inadequate proof
2   that there was limited access?
3   A. My statement is not specific to limitations
4   between the billings department and the laboratory
5   department. My testimony is specific to whether LabMD
6   can specify the types of information that either
7   department has access to.
8   So if you -- if you're not exactly sure what
9   types of information that is required to perform a job
10   or a task, then you can't limit, and that's what I'm
11   saying.
12   I'm not saying -- so whatever information is
13   needed, that's what's needed to do the job, so I'm not
14   saying that laboratory professionals should not have
15   access to information that billings professionals have
16   access to. That's not what I'm trying to say.
17   I'm just saying that if a job is to be
18   performed, that the organization should know what
19   information is needed to perform that job. And that --
20   having that understanding will allow them to put
21   mechanisms in place that will limit that access. That's
22   the only thing that I'm saying.
23   I'm not trying to specify the requirements of
24   information access for the organization and for the
25   employees.

15 (Pages 266 to 269)

270

1   Q. And so it goes back to LabMD's inability to
2   specify, in response to an interrogatory request, what
3   employees had specific access to what information; is
4   that right?
5   A. Yes.
6   JUDGE CHAPPELL: Did you mean interrogatory
7   response?
8   MR. SHERMAN: Excuse me?
9   JUDGE CHAPPELL: Did you mean interrogatory
10   response?
11   MR. SHERMAN: Yes.
12   BY MR. SHERMAN:
13   Q. I would draw your attention to --
14   JUDGE CHAPPELL: I need to make sure the record
15   is clear with the witness. His question said
16   "interrogatory request."
17   Did you take it to mean a request or a response
18   by respondents?
19   THE WITNESS: I took it to mean the response.
20   JUDGE CHAPPELL: Thank you.
21   MR. SHERMAN: Thank you, Your Honor.
22   BY MR. SHERMAN:
23   Q. I'll draw your attention to what's on the screen
24   and submit to you that that is CX 719, which is the
25   testimony of Mr. Robert Hyer.

271

1   Do you recall reviewing testimony of
2   Mr. Robert Hyer?
3   A. Yes.
4   Q. Do you recall as to whether or not Mr. Hyer was
5   also an IT professional who was hired to work for
6   LabMD?
7   A. Yes.
8   Q. And you confirm that he was according to your
9   understanding; correct?
10   A. Yes.
11   Q. If you look at the bottom of page 138, starting
12   at line 22, it reads:
13   "QUESTION: And so following up on that, was it
14   your understanding, based on the way that you
15   configured the servers in the network, that the lab
16   employees could not access the finance information and
17   the financial employees could not access the lab
18   information?"
19   There was an objection interposed there.
20   The answer by the witness: "That -- that was
21   the case before they moved because there were separate
22   servers in separate locations. When they were put
23   together, that separation was a -- an access separation,
24   but it was just as effective."
25   Did I read that correctly?

272

1   A. Yes.
2   Q. Did you review this testimony and consider it
3   before formulating your opinion with regard to whether
4   or not LabMD employees had limited access to information
5   only necessary to perform their jobs?
6   A. Yes, I did.
7   Q. And again, it did not outweigh the reason why
8   you reached your conclusion, which was that LabMD could
9   not specify what information certain employees had
10   access to; correct?
11   A. In addition to the fact that they could not
12   specify, I also used other testimony by IT staff which
13   stated that employees within the billings department was
14   given information that was taken from the overall
15   database that included lab results in order to perform
16   their jobs, so it contradicts this testimony by Mr. Hyer
17   that -- I'm assuming when he says "financial employees,"
18   he's referring to the billing employees, and so
19   individuals within the billings department were given
20   information about information that was generated from
21   the lab testing department, and so there is testimony
22   that actually states this.
23   Now, I'm not saying that that should not occur,
24   because I'm not aware of what information is needed to
25   perform that particular job.

273

1   So there's a contradiction here, so were they
2   never given access, were they given access, the
3   testimony contradicts. The testimony from Mr. Hyer and
4   some of the other testimony that I reviewed basically
5   contradicts, so which then supports the response to the
6   interrogatory request that states that they were given
7   various levels of access to various information.
8   Q. So if it were the case that lab employees
9   needed -- strike that.
10   If it were the case that billing employees
11   needed information from the lab in order to accurately
12   bill the insurance company for the test performed, you
13   would not have a problem with those billing employees
14   having that access; correct?
15   A. No. I would not have a problem with an employee
16   having access to the information that they needed to do
17   their jobs.
18   So there are types of information which looks at
19   specific attributes of the record, and then there is
20   also the amount, the number of records, that an
21   individual would have access to.
22   So if they needed access to all of the
23   attributes within a record to do their jobs, that's what
24   they need. And then an appropriate way to then limit
25   access in that scenario would be to limit the number of

274

1   records that they have access to.
2   So there are various ways to limit access.
3   Q. I want to turn now to page 36 of your report.
4   Are you there?
5   A. Yes.
6   Q. If we look at subparagraph -- well, it's
7   paragraph (c) on that page. It says, "Firewalls were
8   disabled on servers that contained
9   Personal Information."
10   Do you see that?
11   A. Yes.
12   Q. And the footnote is footnote 34, and it refers
13   to the investigational hearing transcript and testimony
14   of Curt Kaloustian.
15   Do you see that?
16   A. Yes.
17   Q. Do you recall that you reviewed the testimony
18   of Mr. Kaloustian in formulating your opinion in this
19   case?
20   A. Yes.
21   Q. And for the proposition that firewalls were
22   disabled on servers that contained personal
23   information, you cite only to Mr. Kaloustian; is that
24   right?
25   A. Yes.

275

1   Q. Were there any other LabMD IT employees that
2   supported this notion that firewall servers -- I'm
3   sorry -- that servers that contained personal
4   information had the firewalls disabled?
5   A. I -- I don't recall. I -- I cannot cite a
6   specific individual.
7   Q. Right.
8   Do you recall if there were any?
9   A. I recall reviewing transcripts that stated that
10   firewalls were disabled on servers, but I don't recall
11   if there were multiple. There could have been, but I
12   can't state exactly.
13   Q. And so the only support that you can exactly
14   state for this proposition is from Mr. Kaloustian whose
15   deposition you reviewed in formulating your opinion.
16   A. For this particular instance, at this moment,
17   yes, that's the only -- that's the one that I cited.
18   Q. Okay.
19   MR. SHEER: Your Honor, may I approach the
20   witness with cough drops?
21   JUDGE CHAPPELL: Sure.
22   MR. SHERMAN: Your Honor, I want to correct
23   something for the record. I referred to
24   Mr. Kaloustian's testimony as deposition testimony when
25   in fact it's civil investigative demand hearing

276

1   testimony.
2   JUDGE CHAPPELL: Okay. You're talking and
3   correcting the source of it but not the question or
4   answer.
5   MR. SHERMAN: That's correct.
6   JUDGE CHAPPELL: All right. That's fine.
7   BY MR. SHERMAN:
8   Q. Also on page 36 of your report, Professor Hill,
9   paragraph (a) indicates that penetration testing was
10   never done.
11   Do you see that?
12   A. Yes.
13   Q. And once again you cite only to Mr. Kaloustian's
14   investigative hearing transcript; correct?
15   A. Yes.
16   Q. Now, that's not exactly true; correct? I mean,
17   we've testified about penetration testing being done in
18   2010.
19   A. Yes, that's not true --
20   Q. Well --
21   A. -- for the -- for all -- for the full relevant
22   time period. Penetration testing was done in 2010.
23   And so I cite Mr. Kaloustian's testimony on that
24   and with regards to the firewalls because if we look at
25   the coverage for IT professionals, there were two main

277

1   IT professionals during the time period that
2   Mr. Kaloustian was there. There was Ms. Alison Simmons
3   and Mr. Kaloustian.
4   And I think that Ms. Alison Simmons' testimony
5   about her responsibilities related more to database
6   maintenance, and Mr. Kaloustian was responsible for
7   firewalls.
8   And so if you look at that testimony during
9   that time period, you would either cite Mrs. Simmons or
10   Mr. Kaloustian and possibly Mr. Maire as it relates to
11   penetration testing, firewall usage and the use of those
12   technical measures.
13   So within that time period, those are the three
14   individuals that you would look at.
15   MS. LASSACK: Your Honor, before we go to -- I'd
16   like to lodge an objection to clarify the record for
17   counsel's prior question.
18   Counsel quoted a subparagraph in
19   Professor Hill's report in paragraph 91, but the prior
20   sentence leading up to that --
21   JUDGE CHAPPELL: Hold on a second. That's what
22   redirect is for.
23   That objection is overruled.
24   If you're saying he misstated something, that's
25   one thing, but if you're trying to bring in something

17 (Pages 274 to 277)

278

1   else in the report, that's for redirect.
2   MS. LASSACK: Your Honor, I was saying that the
3   question was misstated because it was out of context.
4   JUDGE CHAPPELL: "Out of context" is a subject
5   for redirect. If he read it wrong, then we'll clarify
6   that.
7   BY MR. SHERMAN:
8   Q. So you indicated that Mr. Maire was a LabMD
9   employee during the tenure of Mr. Kaloustian, to your
10 understanding?
11   A. Yes.
12   Q. Okay. And Ms. Simmons was a -- was also an IT
13 employee during Mr. Kaloustian's tenure?
14   A. Yes.
15   Q. All right. Can we go to Ms. Simmons'
16 testimony.
17   I would direct your attention to CX 730, which
18 is on the screen, and I will submit to you that that is
19 a portion of Alison Simmons' deposition transcript,
20 which you indicated that she was a contemporary of
21 Mr. Kaloustian; correct?
22   A. Yes.
23   Q. And was it your understanding that
24 Ms. Simmons -- well, whether or not Ms. Simmons had some
25 responsibility for maintaining firewalls?

279

1   A. Can you repeat the question.
2   Q. Is it your understanding as to whether or not
3   Ms. Simmons had some responsibility for maintaining the
4   firewalls at LabMD?
5   A. I'm not exactly sure that she had
6   responsibility. She may have shared some with
7   Mr. Kaloustian. I'm not sure.
8   Q. Do you know whether or not Ms. Simmons was aware
9   of the functionality of the firewalls at LabMD?
10   A. I'm not sure if she was aware of the
11 functionality.
12   Q. Do you know what an HL7 is?
13   A. I think that an HL7 is a specification for
14 data, I think.
15   Q. Do you know whether or not LabMD had an HL7 in
16 place and operating on its system during the relevant
17 period of time?
18   A. I think that they had an HL7 server. Yes.
19   Q. And do you know what the HL7 server is for?
20   A. No. I don't specifically know.
21   Q. Okay. Could we turn to page 13 of Ms. Simmons'
22 deposition, please.
23   The line 5: "Was there anything -- were there
24 any security measures in place that would keep that
25 sharing from happening on LabMD's network?

280

1   "ANSWER: That program wasn't supposed to be on
2   the computer.
3   "QUESTION: But were there any measures in place
4   that would have prevented the sharing from that
5   computer?"
6   I'm sorry. I didn't say "question" and
7   "answer."
8   And what we're talking about here I submit to
9   you is the peer-to-peer sharing.
10   A. Okay. And excuse me. Can you tell me which
11 page and which line you're reading from.
12   Q. I'm sorry. I was reading from page 13.
13   A. Okay.
14   Q. And there was a question -- I'm sorry. Let's go
15 to page 14.
16   Do you recall Ms. Simmons testifying with regard
17 to what occurred after the LimeWire peer-to-peer
18 file-sharing application was found on the computer?
19   A. Do I recall --
20   Q. Do you recall what her testimony said about
21 that?
22   A. I would have to review her testimony to state it
23 specifically.
24   Q. All right. So do you recall whether or not
25 there was a search done by LabMD for LimeWire

281

1   applications on its computers?
2   A. After the sharing had occurred, yes.
3   Q. Well, you're assuming that sharing occurred; is
4   that right?
5   A. Well, I think that that was part of your
6   question; right?
7   Q. Well, not really.
8   A. Oh, okay. So I'm sorry. Could you repeat your
9   question.
10   Q. What they did after they found the LimeWire
11 program on one of their computers.
12   A. I think that they removed the program after they
13 found it.
14   Q. Exactly.
15   Now, if we could turn to page 155, same
16 testimony.
17   If we start at line 11:
18   "QUESTION: Could it have been because there had
19 been an intrusion?"
20   There was an objection interposed there.
21   Line 15:
22   "QUESTION: You know what a I mean by an
23 intrusion?
24   "ANSWER: Possibly, but I think unlikely because
25 I don't -- I think all of those servers were protected

282

1   **by a stronger firewall made to prevent that type of**
2   **intrusion.**
3   **"And I don't think it would have had that type**
4   **of effect. Like I don't think -- I mean this -- every**
5   **single thing, it is like it had been just deleted, so I**
6   **don't think this was the result of an intrusion."**
7   **Did I read that correctly?**
8   A. Yes.
9   **Q. Now, when we're talking about an intrusion,**
10   **we're actually talking about something from the outside**
11   **coming in; is that right?**
12   A. Given the part of the testimony that you've just
13   read --
14   **Q. Yes.**
15   A. -- I'm not exactly sure what specific intrusion
16   that is being referenced here. But I would say that an
17   intrusion is something that is coming from outside of a
18   network, but I'm not sure what -- which intrusion you're
19   referencing here.
20   **Q. Okay. Did you find that in your review, in**
21   **coming to your conclusion, that LabMD, once it found the**
22   **presence of a file-sharing network -- I'm sorry -- a**
23   **file-sharing application on one of its computers, took**
24   **appropriate steps to eliminate that program from its**
25   **computer?**

283

1   A. I found that they removed it in May of 2008.
2   Yes.
3   **Q. And was that very close to the time at which**
4   **they discovered it?**
5   A. That was close to the time that they discovered
6   it but two to three years after it was initially
7   installed. Yes.
8   **Q. Professor Hill, you've indicated in your**
9   **testimony that having policies in writing is very**
10   **important; correct?**
11   A. Yes.
12   **Q. And in coming to your conclusions in this, did**
13   **you review LabMD Employee Handbooks?**
14   A. Yes.
15   JUDGE CHAPPELL: Before you get to that, I have
16   a question.
17   A few moments ago you were talking about an
18   intrusion. I think you said yesterday that if someone
19   downloads a peer-to-peer software product, that's like
20   leaving an open door; correct?
21   THE WITNESS: Yes, sir.
22   JUDGE CHAPPELL: So therefore, if someone
23   accesses the program that employee has downloaded, do
24   you define that as an intrusion?
25   THE WITNESS: I would define that as an

284

1   intrusion because this is an unauthorized piece of
2   software. It is not needed for the business function.
3   And accessing business computers to download
4   information, in making that request and communicating,
5   that I would characterize that as an intrusion. It is
6   not what the business expects to be occurring.
7   JUDGE CHAPPELL: Okay. Thank you.
8   BY MR. SHERMAN:
9   **Q. So is it your testimony, Professor Hill, that**
10   **any unauthorized downloading of software from the**
11   **Internet is an intrusion?**
12   A. It is my testimony that any unauthorized
13   downloading of software presents an opportunity for an
14   intrusion to happen.
15   **Q. Okay. So just because the software was**
16   **downloaded, that does not an intrusion make; correct?**
17   A. That creates the risk and the opportunity for an
18   intrusion.
19   **Q. And so is it your understanding that or is it**
20   **your opinion that because there was a LimeWire software**
21   **downloaded on one computer at LabMD that there was an**
22   **intrusion or there was just the possibility of an**
23   **intrusion?**
24   A. It is my opinion that there's a possibility of
25   intrusion. As I've previously stated, there wasn't

285

1   evidence such as logs that logged the transfer of data
2   that entered and left the LabMD's network for me to make
3   a determination of how that piece of data left the
4   network.
5   **Q. Right.**
6   JUDGE CHAPPELL: I just want to make sure I
7   understand her opinion here.
8   So any unauthorized access of the network would
9   be an intrusion?
10   THE WITNESS: Yes, sir.
11   JUDGE CHAPPELL: So an employee who downloaded
12   the peer-to-peer software is I suppose a co-conspirator
13   to the intruder?
14   THE WITNESS: I wouldn't characterize the
15   person as a co-conspirator, because if they don't have
16   an understanding of the consequences of their actions
17   and -- and -- and what their actions are -- how their
18   actions are going to affect the overall security, I
19   wouldn't -- that's why I wouldn't characterize them as a
20   co-conspirator.
21   But if they didn't download the software, it
22   wouldn't present this opportunity. And also, if they
23   didn't have the ability to download the software, they
24   would not be able to.
25   So there are multiple parties that were

19 (Pages 282 to 285)

286

1   complicit to the downloading of this software, who
2   participated with regards to the downloading. Allowing
3   an employee the ability to do this and giving them that
4   amount of power, you know, allows this to happen.
5   JUDGE CHAPPELL: So if a company policy is that,
6   for example, you can't watch March Madness basketball on
7   the company computer, but somebody watches the first
8   quarter of a game, is that an intrusion?
9   THE WITNESS: If someone watches the first
10   quarter of a game, if -- an intrusion may occur if that
11   video file that they are downloading has some malicious
12   content embedded in it, and they may not know this.
13   JUDGE CHAPPELL: Okay. That's important.
14   Peer-to-peer then is not required. It's just, for
15   example, even a video that you're downloading.
16   THE WITNESS: Even a video that you're
17   downloading may contain some malicious content. That's
18   why it's always important to understand how your actions
19   may affect the network.
20   An individual may think that, oh, I'm just
21   watching a video. They don't think about the fact that
22   this video may have embedded malicious content.
23   So when you're doing things that do not adhere
24   to what is required to perform your job, you put that
25   infrastructure at risk.

287

1   JUDGE CHAPPELL: All right. So just so I'm
2   clear on your definition, a spam e-mail comes into the
3   company e-mail account. An employee opens it, but they
4   don't click on, let's say, the malicious attachment. Is
5   that an intrusion?
6   THE WITNESS: The intrusion -- the spam e-mail
7   presents an opportunity for an intrusion to occur. If
8   they don't click on the malicious content, then that
9   risk is not executed. That risk of an intrusion does
10   not occur.
11   JUDGE CHAPPELL: So am I correct then that your
12   opinion would be, any time there's Internet access,
13   there's the possibility of intrusion?
14   THE WITNESS: Any time that there's Internet
15   access, there is a possibility of an intrusion.
16   JUDGE CHAPPELL: Or even e-mail, outside
17   e-mail.
18   THE WITNESS: Outside e-mail.
19   And so that's why you want to have policies in
20   place and enforcement mechanisms to limit what an
21   employee can do.
22   JUDGE CHAPPELL: Okay. Thank you.
23   BY MR. SHERMAN:
24   Q. I think I may have asked this, but I want to
25   make sure it's clear, that the downloading of LimeWire

288

1   onto the desktop at LabMD, you do not consider that an
2   intrusion but a possibility, opening the possibility
3   that an intrusion may occur; correct?
4   A. Yes. It opens up the possibility that an
5   intrusion may occur and not with regards to the LimeWire
6   application, not just with the use of the application,
7   but the software itself may have malicious components
8   embedded in it.
9   Q. I think my last question was whether or not you
10   had looked at LabMD's Employee Handbook, and if -- we're
11   going to direct your attention to RX 71.
12   Would you like for us to enlarge that for you or
13   can you see it?
14   A. Can you enlarge it slightly, please.
15   Q. Can you enlarge it, please.
16   A. Okay.
17   Q. The part I want you to look at is Personal Mail,
18   E-Mail and Phone Calls.
19   Do you see that section?
20   A. Yes, I do.
21   Q. The second paragraph under that heading reads,
22   "Personal Internet or e-mail usage in the office is
23   prohibited. This policy stands at all times, even when
24   an employee is on a lunch period. Computers in the
25   office are property of LabMD and should only be used for

289

1   company-related reasons."
2   Did I read that correctly?
3   A. Yes.
4   Q. Is this one of the -- if you look down at the
5   bottom also of the page -- can we scroll to the
6   bottom -- it says "revised June 2004."
7   Do you see that?
8   A. Yes.
9   Q. Is this one of the LabMD handbooks that you
10   reviewed?
11   A. Yes.
12   Q. Okay. Now, Professor Hill, do you consider
13   what's written in the handbook here to be policies of
14   the company?
15   A. I consider this to be a policy.
16   Q. Okay. And so you would agree then that, at
17   least according to this, as early as 2004 that there was
18   a policy at LabMD that prohibited Internet use and
19   e-mail uses for personal reasons; is that correct?
20   A. Yes.
21   Q. You would also agree that there was a policy
22   that computers in the office were property of LabMD and
23   that they should only be used for company-related
24   reasons; correct?
25   A. Yes.

20 (Pages 286 to 289)

290

1   Q. Okay. You would also agree then that this would
2   affect in fact security, the data security of the
3   company, if this policy were followed, it would in fact
4   have an impact on data security for the company;
5   correct?
6   A. What I can say about this particular policy,
7   that as it is written, it is not sufficient to satisfy
8   a security goal because there's no discussion or
9   presentation of how this policy would actually satisfy
10   a specific security goal and what goal is to be
11   satisfied.
12   So there is no link to the overall security
13   goal, so an employee doesn't understand the
14   consequences that violating this policy would have on
15   security.
16   So as I've previously stated, when defining
17   policies for a comprehensive security plan, you have to
18   link your security goals to the policy, so -- and the
19   policy then to the mechanisms that would enforce that.
20   And so in the -- with this presentation of it
21   in an employee handbook, this would not be sufficient
22   to communicate a security policy for employees. This
23   would sufficiently communicate a business policy. But
24   an individual doesn't -- wouldn't necessarily understand
25   the security implications of violating this policy, so I

291

1   can't say that this policy would protect data, because
2   you need that overall connection between the goals that
3   are to achieve and an explanation to the employees about
4   that.
5   Q. If the policy were followed to the letter with
6   regard to Internet and e-mail usage, would that have a
7   positive impact on the data security of the company?
8   A. Yes. If this policy was followed and there were
9   no violations, it would have a positive impact.
10   Q. Do you consider the fact that -- and we can skip
11   down to the paragraph two paragraphs below that, where
12   it reads, "You will be reprimanded for failure to comply
13   with this policy."
14   Is that sufficient to communicate a consequence
15   of violating the policy?
16   A. It communicates a consequence but not a security
17   consequence or the consequences to the overall security
18   of the organization --
19   Q. And the last sentence of that same paragraph
20   says, "A combination of phone calls or e-mails may
21   result in immediate termination."
22   Did I read that correctly?
23   A. Yes.
24   Q. Is that sufficient to communicate a consequence
25   of violating the policy?

292

1   A. As I have previously stated, it communicates a
2   consequence, but not the consequences and the
3   implications of how a violation would affect the overall
4   security of the organization's computing infrastructure
5   and the data that's maintained within that
6   infrastructure.
7   Q. Let's turn to page 9 of this same document.
8   There's a heading on that page called Security.
9   Would you enlarge that.
10   Do you see that, Professor Hill?
11   A. Yes, I do.
12   Q. Under Security, it reads, "When LabMD facilities
13   are equipped with electronic security systems, access to
14   the buildings before and after normal working hours may
15   be achieved on a limited basis only. Should you be
16   required to work during hours other than normal working
17   hours, you must call someone who will allow you access
18   or make arrangements in advance of hours needing
19   access."
20   Would you consider this as beneficial in terms
21   of securing a company's data, in terms of securing a
22   company's information, to have this type of security
23   policy in place?
24   A. Yes. This follows the principle of physical
25   security that I provided as a part of a comprehensive

293

1   information security program, so this addresses the need
2   for physical security.
3   Q. And in fact, it's your opinion that LabMD's
4   physical security was adequate; is that correct?
5   A. Yes. As far as providing locks to server rooms
6   and access to their -- physical access to their
7   computers, yes. But physical security is not sufficient
8   in protecting against electronic attacks.
9   Q. Right.
10   And I think you also said that no one portion of
11   your seven principles alone would meet your definition
12   of a comprehensive information security program;
13   correct?
14   A. No one of the seven principles would meet the
15   definition of any of the organizations' that I've cited
16   notion of a comprehensive information security plan.
17   Q. If we look down at the bottom of that page,
18   under LabMD Property --
19   A. Excuse me. Could you reduce that just slightly.
20   It's not fitting fully on the screen.
21   Okay. I'm able to see it now.
22   Q. Again, under LabMD Property, it reads: Lockers,
23   desks, vehicles and computers are all office equipment
24   are LabMD's -- and all office equipment -- I'm sorry --
25   are LabMD's property and must be maintained according to

21 (Pages 290 to 293)

294

1   LabMD's standards, rules, and regulations. They must be
2   kept clean and operable and are to be used only for
3   work-related purposes.
4   Professor Hill, do you think that this is a
5   beneficial policy to have in place with regard to
6   security of data that might be contained on computers
7   and other property maintained by the -- by LabMD?
8   A. As I've previously stated regarding policies,
9   there is no link in this statement to a consequence as
10 it relates to the security of the system and how
11 violating this policy would impact the overall
12 security.
13   So as we previously stated, if this is followed
14 to the letter in that if employees don't do anything to
15 violate this, then I think that it would be helpful.
16   Q. The next paragraph reads, "Employees who need to
17 remove LabMD property, equipment, records or information
18 from the premises must have proper authorization.
19 Removal and/or possession without this authorization is
20 prohibited and subject to disciplinary action up to and
21 including termination."
22   Professor Hill, once again, if this policy is
23 followed to the letter, would that not be beneficial in
24 terms of securing data and information and property of
25 the company?

295

1   A. Yes, it would.
2   Q. Professor Hill, we've talked a lot about this
3   comprehensive information security program. We've
4   talked about the seven principles.
5   Is there anything that LabMD could have done
6   short of meeting every goal you set out in your opinion
7   and still have you find that their data security was
8   adequate?
9   A. The recommendations that I laid out in my expert
10 witness document contain basic requirements for securing
11 a system. These are consistent with recommendations by
12 governmental and industry and academic institutions
13 working together to define and specify such
14 recommendations.
15   So it is expected that an organization will
16 apply updates to their software. It is expected that
17 they will have strong passwords. It would -- it is
18 expected that they would implement access control
19 mechanisms. It is expected that they would assess their
20 networks for emerging vulnerabilities.
21   So what I've recommended is what these other
22 guidelines recommend. These are the basic things that
23 you must do to have reasonable and appropriate security
24 for your system.
25   So I don't think the guidelines that I've put in

296

1   place exceed what the other guidelines by those
2   organizations are recommending. For both -- for small
3   organizations and for large organizations, the
4   guidelines are consistent.
5   Q. And I guess my question is a little different
6   than your answer.
7   My question is whether or not LabMD could have,
8   in your opinion, had in place adequate data security
9   without meeting every aspect of your recommendation.
10   A. The -- I'll try to answer your question this
11 way.
12   The majority of the recommendations that I made
13 were in response to me determining that there were
14 multiple vulnerabilities and flaws and limitations to
15 the existing security plan that they had, so here I'm
16 trying to address these vulnerabilities.
17   So if there are vulnerabilities in the existing
18 plan, they need to be addressed in order to have
19 appropriate and reasonable security, and so this relates
20 to what they were currently doing but not doing
21 sufficiently and effectively, and so they would need to
22 address those vulnerabilities.
23   Q. And they would need to address those
24 vulnerabilities in the way that you suggested that they
25 address them in order to -- in order for you to conclude

297

1   that their data security was adequate.
2   A. I think I gave some general recommendations.
3   There's a general recommendation for risk
4   assessment and for it to be performed periodically.
5   Now, there are various mechanisms for doing risk
6   assessment, and the coverage of those mechanisms are
7   different, and so of course they would need antivirus
8   software, but which antivirus software I don't specify.
9   So they would need to do some types of
10 penetration testing and vulnerability assessment, so --
11 and there are a variety of different mechanisms for
12 doing that. But my general recommendation is that they
13 do risk assessment, and so there are different
14 mechanisms for doing that. And I don't specify that,
15 you know, you've got to use this explicit one or that
16 explicit one, but I do give examples of the types that
17 they should use in order to address this.
18   So there is -- in my recommendation, LabMD has
19 some leeway with regards to, you know, how to address
20 the vulnerabilities given the recommendations that I
21 have put in place.
22   Q. Just a few more questions with regard to
23 policies that were in place at LabMD.
24   If we could turn to CX 2, which I believe you
25 were questioned about yesterday and should be in the

298

1   folder that you have on your lap.
2   If we could go to page 5.
3   Page 5, please, Professor Hill.
4   Professor Hill, you were originally at the cover
5   page of CX 2, and I think yesterday you established that
6   this in fact was also part of what you reviewed in
7   coming to your conclusions and your opinions in this
8   case; correct?
9   A. Yes.
10   Q. And as far as page 5 is concerned, if we can go
11   down to Confidentiality and Trade Secrets?
12   A. Yes.
13   Q. It reads, "In the course of your work, you may
14   have access to confidential information regarding LabMD,
15   its suppliers, customers, operations methods, current or
16   potential products, or services and software used at
17   LabMD. It is one of your most serious responsibilities
18   that you in no way reveal or divulge any such
19   information and that you use information only in the
20   performance of your duties, as certain information could
21   be used by competitors. Violation of this may subject
22   you to immediate termination."
23   Professor Hill, do you agree that if this policy
24   is followed that it would have a positive impact on data
25   security at LabMD?

299

1   A. Yes. If this policy was followed, it would have
2   a positive impact.
3   Q. And you -- well, I'm going to ask the obvious
4   question. I don't mean to offend you.
5   But this policy is in writing, wouldn't you
6   agree?
7   Professor Hill?
8   A. This policy is in writing. But as I've
9   previously stated, a policy alone without an
10   enforcement mechanism is not sufficient.
11   And -- and the reason -- one of the reasons that
12   I say an enforcement mechanism is important and also a
13   training and discussion is important, because an
14   individual may do something that may inadvertently
15   violate this policy that they don't have an
16   understanding that it will.
17   For example, downloading unauthorized software,
18   they don't directly share or give that information away,
19   and they may not be aware that they're doing it.
20   So while this policy talks about, you know,
21   directly sharing and intentionally sharing information,
22   it doesn't cover the case where information may be
23   inadvertently shared because of the actions of an
24   employee that doesn't understand the security
25   consequences or the consequences to security of doing

300

1   that particular action.
2   Q. If we could turn to page 6, which is the next
3   page, at the top.
4   It reads, "The Health Insurance Portability and
5   Administrative Act (HIPAA) of 1993 made it illegal for
6   any person in healthcare to share an individual's
7   protected healthcare information (PHI) with anyone other
8   than for the specific reasons of treatment, payment, or
9   healthcare operations."
10   Again, Professor Hill, if this written policy is
11   followed, it would have a positive impact on data
12   security as it relates to protected health information,
13   wouldn't it?
14   A. Yes, it would.
15   Q. Now, Professor Hill, you've discussed and stated
16   repeatedly that how important it is to have policies in
17   writing; correct?
18   A. It's important to have your entire comprehensive
19   information security plan in writing.
20   Q. It's important --
21   JUDGE CHAPPELL: Mr. Sherman, you're the
22   examining attorney, but would you like for the witness
23   to answer merely yes or no when you've asked a yes-or-no
24   question?
25   MR. SHERMAN: Your Honor, I respect

301

1   Professor Hill's opinion and -- her voice is tired. You
2   would think that she would want a yes or no answer,
3   but -- that is an option, Professor Hill.
4   THE WITNESS: Okay.
5   MR. SHERMAN: I think that's what the judge is
6   suggesting.
7   BY MR. SHERMAN:
8   Q. You've also indicated time and again that
9   guidelines should be in writing; correct?
10   A. Yes.
11   Q. And you've stated that the reason that it's so
12   important for these to be in writing is because it
13   creates awareness amongst not only IT professionals but
14   also the employees who are expected to comply; correct?
15   A. Yes.
16   Q. That it creates continuity in terms of the
17   enforcement and knowledge of those policies as turnover
18   may occur; correct?
19   A. Yes.
20   Q. So, Professor Hill, do you think that it's
21   important or just as important for an enforcement agency
22   to put its data security expectations in writing for the
23   very same reasons?
24   A. Excuse me. Did you say enforcement agency?
25   Q. Yes. Such as the FTC, the government.

23 (Pages 298 to 301)

302

1   A. I think -- yes.
2   MR. SHERMAN: If I can have one moment to
3   consult with counsel.
4   JUDGE CHAPPELL: Go ahead.
5   (Pause in the proceedings.)
6   BY MR. SHERMAN:
7   Q. Just a few more questions.
8   In terms of LabMD, were you aware of what type
9   of services LabMD provided?
10   A. During the relevant time period?
11   Q. Yes, ma'am.
12   A. Yes.
13   Q. And what were they? What did you know?
14   A. I knew that they provided testing for doctors'
15   offices for different types of lab tests.
16   Q. Did you know that they specified or specialized
17   in cancer detection?
18   A. I didn't know that specifically, no.
19   Q. Did you know that LabMD received the protected
20   health information -- did you know how they received
21   that information from their physician clients?
22   A. Yes.
23   Q. And did you know how the physician clients
24   received their test results from LabMD?
25   A. Yes.

303

1   Q. And were you aware of whether or not the federal
2   government had in fact encouraged medical care providers
3   to go electronically as it related to medical records,
4   during the relevant period of time?
5   A. Yes.
6   Q. You were aware of that.
7   A. Yes.
8   Q. Now, Professor Hill, we haven't gone into your
9   background in terms of your previous employment, but we
10   did so at your deposition, and I'll try and make this
11   short.
12   When was the last time you actually worked in
13   the private sector?
14   A. I would have to take a look at my CV to --
15   Q. Please do.
16   (Pause in the proceedings.)
17   A. I would say that it was in 1999.
18   Q. Okay. And since 1999, you've been an academic
19   professor --
20   A. Yes.
21   Q. -- is that correct?
22   Have you been asked, other than for this case,
23   to provide consulting services for any ongoing and
24   operating business with regard to their data security?
25   A. No.

304

1   Q. Have you looked at specifically the operations
2   of any medical facilities, whether it be doctors'
3   offices, hospitals, laboratories like LabMD, in order to
4   look at their operations and recommend data security
5   practices for them?
6   Medical facilities.
7   A. I would need to qualify my answer if that's
8   okay.
9   Q. Absolutely.
10   A. As a part of research that I've conducted, I
11   have looked at the activities of hospitals and their use
12   of RFID technology to understand what the privacy
13   implications of the use of that technology would be on
14   the patient. And I've interviewed doctors along with
15   the students that I've worked with in order to get an
16   understanding of the process of using that within that
17   hospital environment in order to assess the risk and
18   proposed mechanisms for securing the use of such
19   technology.
20   Q. Was that study part of a grant or was that --
21   A. No. This is prior to trying to secure a grant
22   to continue that work.
23   So no, it wasn't as part of grant-related work.
24   Q. How long ago was this?
25   A. This was, if I can --

305

1   Q. Absolutely.
2   A. This work was conducted between 2008 and 2009.
3   Q. And it specifically addressed RFID technology?
4   A. Yes.
5   Q. What is RFID technology?
6   A. RFID technology is radiofrequency
7   identification. And you have a small computing chip
8   that emits radiofrequencies in order to communicate
9   information, so some of these chips can be as simple as
10   an electronic barcode or it could be a programmable chip
11   where you can recode information and store additional
12   information on the chip itself.
13   MR. SHERMAN: Thank you, Professor Hill.
14   I have no further questions, Your Honor.
15   JUDGE CHAPPELL: Any redirect based on the
16   cross-exam?
17   MS. LASSACK: I do, Your Honor.
18   May we take a lunch break?
19   JUDGE CHAPPELL: I have a few questions before
20   your redirect.
21   I heard you talk a lot about defense in depth.
22   Is "defense in depth" your lingo created by
23   you?
24   THE WITNESS: No, sir.
25   JUDGE CHAPPELL: Where is it from?

24 (Pages 302 to 305)

306

1   THE WITNESS: "Defense in depth" is a term
2   that's used in the IT community and -- and it is my
3   understanding that it was originally taken from
4   military strategy, but it has been adopted by the IT
5   community to explain the most effective way to deploy
6   mechanisms.
7   JUDGE CHAPPELL: When do you believe you first
8   saw that use of that phrase as commonplace in the
9   IT community?
10   THE WITNESS: I --
11   JUDGE CHAPPELL: I mean, you don't have to --
12   like five years, ten years, one year, how long ago?
13   THE WITNESS: I think that it was maybe around
14   five years ago or so when I became familiar with the
15   strategy.
16   JUDGE CHAPPELL: And the seven principles
17   you've talked about, is that your formulation? Even
18   though I think you said they were drawn from various
19   literature or guidelines, did you formulate the seven
20   principles?
21   THE WITNESS: No, sir. These are principles
22   that I've learned through my experience. And these are
23   consistent with what may be found in the guidelines
24   that are provided by some of the resources that I cite.
25   JUDGE CHAPPELL: Did I hear you say earlier that

307

1   you generally won't find all seven if you look at
2   guidelines or information?
3   THE WITNESS: You may not find all seven
4   specifically. You may find six, excluding the
5   "don't keep what you don't need," because since the
6   management of large amounts of data is an emerging
7   trend, then this is becoming more of a needed principle
8   because of that, because organizations are keeping
9   large amounts of money, so you may not see that
10   particular principle in some of the documents that I
11   cite.
12   JUDGE CHAPPELL: Is it your opinion that
13   respondent's data was unreasonable or inadequate simply
14   because it didn't meet standards for defense in depth?
15   THE WITNESS: I feel that it was because not
16   just because it didn't meet standards for defense in
17   depth but because they were not comprehensive and that
18   they had vulnerabilities that were not being addressed
19   because of the lack of specific policies and enforcement
20   mechanisms.
21   JUDGE CHAPPELL: Just so I'm clear, defense in
22   depth, does that require a company to meet the seven
23   principles?
24   THE WITNESS: Defense -- it doesn't require the
25   companies to meet the seven principles, but it's more

308

1   of a strategy about how to deploy mechanisms within
2   your computing infrastructure, mechanisms and policies,
3   in order to satisfy your security goals.
4   So you have this comprehensive information
5   security plan that lists out, you know, what mechanisms
6   will enforce your policies and satisfy your security
7   goals, but defense in depth talks about you need a
8   heterogeneous set of mechanisms, not the same. You need
9   to deploy them at multiple layers in your network in
10   order for them to be effective.
11   So that's what defense in depth says --
12   JUDGE CHAPPELL: So -- go ahead.
13   THE WITNESS: -- so --
14   JUDGE CHAPPELL: I didn't mean to interrupt you.
15   Go ahead.
16   THE WITNESS: Okay.
17   So you have this plan that you devise via a
18   process of kind of a balancing process where you look at
19   your goals and look at the highest risks and
20   vulnerabilities, and you identify mechanisms that will
21   address those that you're more likely to encounter with
22   regards to the risk and the vulnerabilities that would
23   be exploited. And then given that, you want to then
24   deploy those mechanisms in a defense in depth way.
25   So that's how defense in depth kind of fits with

309

1   this comprehensive information security program.
2   JUDGE CHAPPELL: So if I understand correctly,
3   defense in depth would be considered the gold standard
4   in the industry.
5   THE WITNESS: I wouldn't say that defense in
6   depth is a gold standard. It's an effective strategy.
7   JUDGE CHAPPELL: I think it's paragraph 52 of
8   your expert report says -- you're talking about best
9   practices that would include seven principles. And I'm
10   just trying to follow you here.
11   If someone follows the seven principles, are
12   they meeting what you would consider defense in depth,
13   that requirement?
14   THE WITNESS: If someone follows those seven
15   principles and deploy mechanisms at the various levels
16   within their infrastructure, then they would satisfy
17   defense in depth.
18   JUDGE CHAPPELL: And again so I'm clear, is
19   defense in depth, in your opinion, the exercise of
20   utmost care, in other words, above reasonable care?
21   THE WITNESS: I'm sorry, Your Honor. Could you
22   repeat.
23   JUDGE CHAPPELL: Defense in depth, is that
24   exercising reasonable care or is it more likely what you
25   would call or consider utmost care?

310

1   THE WITNESS: I would say it's reasonable, sir.
2   JUDGE CHAPPELL: So in your opinion then,
3 reasonable care would be defense in depth for your
4 network.
5   THE WITNESS: Reasonable care would be defense
6 in depth.
7   JUDGE CHAPPELL: Okay. Thank you.
8   We will take our lunch break.
9   How much time do you think you'll need for
10 redirect?
11   MS. LASSACK: Under half an hour, probably
12 closer to 15 minutes.
13   JUDGE CHAPPELL: Okay. We'll reconvene at
14 2:10 p.m.
15   We're in recess.
16   (Whereupon, at 1:03 p.m., a lunch recess was
17 taken.)
18
19
20
21
22
23
24
25

311

1   A F T E R N O O N   S E S S I O N
2   (2:12 p.m.)
3   JUDGE CHAPPELL: Back on the record.
4   Redirect?
5   MS. LASSACK: Thank you, Your Honor.
6   - - - - -
7   REDIRECT EXAMINATION
8   BY MS. LASSACK:
9   **Q. Good afternoon, Professor Hill.**
10   A. Good afternoon.
11   **Q. I'd like to start by directing your attention to**
12 **paragraph 91 of your expert report, which is labeled**
13 **CX 740, and which begins on page 35.**
14   **Mr. Sherman asked you this morning about the**
15 **subparagraphs of paragraph 91, which begin on the**
16 **following page, page 92. Do you remember that?**
17   A. Yes.
18   **Q. To clarify the record, the opinions in**
19 **paragraphs 91 (a) through (g) of your report are true**
20 **for what time period?**
21   A. Prior to 2010.
22   **Q. Professor Hill, you testified this morning about**
23 **intrusions. Do you recall that testimony?**
24   A. Yes.
25   **Q. In giving that testimony, how are you defining**

312

1 **the word "intrusion"?**
2   A. The way that I'm defining the word "intrusion"
3 is that an intrusion is unauthorized access that
4 originates from outside of a network.
5   **Q. When you say "unauthorized," unauthorized from**
6 **whose perspective?**
7   A. Unauthorized from the perspective of the
8 organization.
9   **Q. Professor Hill, you also testified this morning**
10 **that there were not sufficient logs to show how the**
11 **1718 File left LabMD. Do you recall that testimony?**
12   A. Yes.
13   **Q. Would you please explain to the court what you**
14 **mean by that.**
15   A. There were no -- there was no information
16 regarding the data communication that occurred that
17 allowed that file to leave the network.
18   For example, if you had mechanisms in place to
19 capture the data across the network, then you could
20 possibly have information that would be able to tell you
21 how the file left the network.
22   So when I say "logs," I'm talking about
23 information, data communication information, the data
24 that transferred between the external entity and LabMD's
25 network.

313

1   **Q. So that information was not available in this**
2 **case?**
3   A. No, it was not available.
4   **Q. Professor Hill, you testified this morning about**
5 **certain LabMD policies and LabMD's employee manual. Do**
6 **you recall that testimony?**
7   A. Yes.
8   **Q. In your expert opinion, is it reasonable to**
9 **expect employer policies like the ones you testified**
10 **about this morning to be followed to the letter?**
11   A. It's not reasonable to expect them to be
12 followed to the letter.
13   **Q. Why not?**
14   A. Because there can always be human error.
15   And so the human is the weakest part of any
16 security plan, and so there could be a misunderstanding
17 of the policy, there could be misconfigurations of
18 mechanisms, and so there can always be an unintentional
19 mistake on the part of the human that would prevent a
20 policy from being followed to the letter. I think it's
21 unreasonable to expect that.
22   **Q. Professor Hill, you also testified this morning**
23 **that a company should be able to specify what types of**
24 **information that its employees have access to. Do you**
25 **recall that testimony?**

26 (Pages 310 to 313)

314

1   A. Yes.
2   Q. Can you explain to the court why you believe
3   that a company should be able to specify the types of
4   information that its employees have access to?
5   A. There are specific tasks that a company
6   performs, and there should be knowledge of what is
7   required to perform those tasks. And if that knowledge
8   is not documented, it would still be possible to
9   determine what that knowledge is based on the
10 applications that are in place and the information that
11 is provided through those applications.
12   So I think it should be possible for a company
13 to specify that for those reasons.
14   Q. When you say "by the applications," can you
15 explain to the court what you mean by that.
16   A. The application, for example, the billing
17 application Lytec provided certain information and
18 provided access to certain information, and so that
19 would -- that application could then be used to
20 determine what the billings application provided access
21 to.
22   There's been testimony that stated that the
23 billings employees needed additional information from
24 the database, so there are processes in place to extract
25 this information, and so those processes should be

315

1   evaluated to determine what information was extracted in
2   addition to the billings information.
3   So there's a way to recover that information by
4   evaluating the processes that are in place at an
5   organization.
6   Q. Professor Hill, I'd like to direct your
7   attention to paragraph 38 of your expert report.
8   And I apologize. I misspoke. Actually I'd like
9   to direct your attention to paragraph 49 of your expert
10 report.
11   You testified earlier this morning about the
12 last sentence of that paragraph. Do you recall that
13 testimony?
14   A. Yes.
15   Q. Will you read the last sentence of
16 paragraph 49 aloud.
17   A. "For purposes of this report, I have assumed
18 that these types of information can be used to harm
19 consumers, through identity theft, medical identity
20 theft, and disclosing private information."
21   Q. To clarify the record, did you make any
22 assumptions about consumer harm in this case beyond what
23 you just read?
24   A. No, I did not.
25   Q. Professor Hill, you explained to the court

316

1   yesterday that LabMD failed to provide reasonable and
2   appropriate security to protect the personal
3   information --
4   JUDGE CHAPPELL: Hold on a second. You referred
5   to her testimony yesterday? That would have been
6   direct. Your redirect is limited to the scope of cross,
7   so don't go beyond the scope of cross that we heard
8   today.
9   MS. LASSACK: Okay. I don't believe that I am,
10 Your Honor. May I continue --
11   JUDGE CHAPPELL: Well, I just heard you start by
12 saying you testified yesterday. Yesterday was direct,
13 not cross, so you need to change your question.
14   MS. LASSACK: Okay. I can rephrases the
15 question.
16   BY MS. LASSACK:
17   Q. Professor Hill, you've just testified that
18 you -- the only assumption you made about consumer harm
19 in this case is the assumption that you just read from
20 paragraph 49 of your report --
21   A. Yes.
22   Q. -- correct?
23   Do you have any opinion about whether LabMD's
24 failure to provide reasonable and appropriate data
25 security increased the risk that the personal

317

1   information it maintained on its network could be
2   disclosed without authorization?
3   MR. SHERMAN: Objection.
4   JUDGE CHAPPELL: Basis?
5   MR. SHERMAN: I don't believe that
6   Professor Hill's background, experience, education
7   qualifies her to give an opinion with regard to likely
8   harm. I think that was the question that was asked.
9   JUDGE CHAPPELL: Is this opinion that this
10 question is seeking within her expert report?
11   MS. LASSACK: I believe that it is, Your Honor.
12 The question is about the risk of unauthorized
13 disclosure, and I believe Professor Hill testifies about
14 that in her report in connection with defense in depth
15 and --
16   JUDGE CHAPPELL: Then you need to -- based on
17 the objection, you need to lay a foundation.
18   Meaning you need to have the witness testify
19 that this is an opinion previously provided in her
20 report. She's limited to those opinions in this
21 proceeding. That's the foundation that's required.
22   MS. LASSACK: Thank you, Your Honor.
23   BY MS. LASSACK:
24   Q. Professor Hill, did you offer an opinion in your
25 report about the increased risk that not having

27 (Pages 314 to 317)

318

1   reasonable and appropriate data security would create
2   with respect to the chance of unauthorized disclosure of
3   that information?
4   A. Yes.
5   Q. So will you please explain to the court what
6   that opinion is.
7   A. That opinion is, given the vulnerabilities that
8   were present within LabMD's computing infrastructure and
9   the fact that they were not addressed in a timely
10 manner, this placed the personal information that was
11 stored on those networks at risk for exposure and
12 compromise.
13   Q. Is that risk greater than the risk would be if
14 LabMD had provided reasonable and appropriate security?
15   A. Yes.
16   Q. What is the basis for that opinion?
17   A. The basis of that opinion is that if they had
18 provided reasonable and appropriate security, the
19 high-level risk would have been identified and
20 addressed, and those vulnerabilities would not have
21 been present for the duration of the relevant period,
22 and so that's why, that the increased level of
23 exposure, the type of risks that were present, the fact
24 that those risks gave an attacker administrative access
25 to servers that maintained the sensitive information,

319

1   that's why I feel that there was increased risk to that
2   data.
3   MS. LASSACK: I have no further questions,
4   Your Honor.
5   JUDGE CHAPPELL: Thank you.
6   Is there any recross based on the redirect
7   only?
8   MR. SHERMAN: There is recross, Judge.
9   - - - - -
10   RECROSS-EXAMINATION
11   BY MR. SHERMAN:
12   Q. Professor Hill, could you turn to your report
13 and point to me where in that report you state that
14 there's an increased risk of data exposure as a result
15 of LabMD's data security practices.
16   (Pause in the proceedings.)
17   JUDGE CHAPPELL: If it would help, counsel may
18 confer, and if that information is not in the report, we
19 can establish that and move along.
20   MR. SHERMAN: I don't think it's in the report,
21 Your Honor, and if it's not, I would move to have
22 the --
23   JUDGE CHAPPELL: Well, don't -- we're not there
24 yet.
25   MR. SHERMAN: Well, do you find it, Counsel?

320

1   MS. LASSACK: I think I can establish that
2   there are risks that cause harm and that when defense in
3   depth --
4   JUDGE CHAPPELL: All I want to hear from you,
5   Counselor, is I want to know the page and line number
6   where it's in her report. That's the question. Not the
7   page, not the line number, but the paragraph number,
8   where is it in her report.
9   MS. LASSACK: I think that's paragraph 76,
10 paragraph 100(d), and paragraph 27 read together, would
11 be that opinion.
12   JUDGE CHAPPELL: Can someone give me a copy of
13 the report, please.
14   MS. LASSACK: May I approach, Your Honor?
15   JUDGE CHAPPELL: Yes.
16   MS. LASSACK: Thank you.
17   JUDGE CHAPPELL: Thank you.
18   (Pause in the proceedings.)
19   Dr. Hill, have you found that wording in your
20 report?
21   THE WITNESS: Your Honor, when looking at --
22   JUDGE CHAPPELL: I'm not talking about reading
23 paragraphs together. This is a concluding -- a
24 conclusion that should be stated as worded in this
25 question. Is that in your report?

321

1   THE WITNESS: I haven't found it worded like it
2   was in the question, sir.
3   JUDGE CHAPPELL: Do you need more time?
4   THE WITNESS: I can continue to look, but I
5   haven't found it stated exactly.
6   JUDGE CHAPPELL: Do you recall it being in
7   there?
8   THE WITNESS: I don't recall it being in there
9   stated exactly like the question, sir.
10   JUDGE CHAPPELL: Do we have an objection?
11   MR. SHERMAN: You do, Your Honor. I would
12 object to the testimony in that regard and ask that it
13 be stricken.
14   JUDGE CHAPPELL: I have reviewed the paragraphs
15 cited into the record by complaint counsel, 100(d), 27,
16 and 76 read together.
17   First off, the paragraphs should not have to be
18 read together to try to find an opinion. It should be
19 clear, concise and obvious in an expert report.
20   First of all, I find that it's not in the
21 report.
22   Second of all, I find that reading those
23 paragraphs together does not equal the opinion the
24 question called for.
25   Therefore, any response from this witness

28 (Pages 318 to 321)

322

1   regarding that question and that opinion will be
2   disregarded and not considered in the decision on this
3   case.
4   And just to be clear for the record, the
5   question was: "Professor Hill, could you turn to your
6   report and point to me where in that report you state
7   that there's an increased risk of data exposure as a
8   result of LabMD's data security practices."
9   Next question.
10   The objection is sustained.
11   MR. SHERMAN: Thank you, Your Honor.
12   JUDGE CHAPPELL: I want to make it clear in the
13   record that any testimony saying there was an increased
14   risk, based on my previous finding, will be disregarded
15   and not considered as part of the decision in this
16   case.
17   I find it patently unfair to introduce a new
18   opinion in this case. That's we why we have the rules.
19   That's why we have expert opinions. Those opinions are
20   what this case is limited to, the opinions in the expert
21   report.
22   Next question.
23   MR. SHERMAN: Thank you, Your Honor.
24   BY MR. SHERMAN:
25   Q. Professor Hill, you testified that the relevant

323

1   time period was 2005 through 2010; correct?
2   A. Yes.
3   Q. And on redirect you were asked questions about
4   the inability to discern how the documents allegedly
5   escaped LabMD's possession; correct?
6   A. I'm sorry. I -- I don't know when that question
7   was asked, but if you're stating that it was asked
8   during that time, then --
9   Q. Well, redirect was when Ms. Lassack was just
10   talking to you a few moments ago.
11   A. Yes.
12   Q. Do you recall that question being asked in that
13   time frame in terms of your ability to, through logs or
14   through information that you reviewed, determine how
15   certain information escaped LabMD's possession?
16   A. I honestly don't recall her asking me that
17   question, but I can answer anything that you're asking.
18   Q. You indicated that there weren't sufficient logs
19   to make that determination.
20   A. Oh, logs. Okay. I heard "laws."
21   Q. Oh, I'm sorry. No. Logs.
22   A. Yes. Okay. Yes.
23   Q. To make that determination.
24   A. Now I understand. I'm sorry.
25   Q. My apologies for not being clear.

324

1   There weren't sufficient logs to make that
2   determination.
3   A. Yes.
4   Q. Okay. But there were logs being run during that
5   period of time; isn't that correct?
6   A. It is my understanding that there weren't the
7   types of logs that I was referring to.
8   Q. And -- okay.
9   No further questions.
10   JUDGE CHAPPELL: Is there any re-redirect based
11   on the recross?
12   MS. LASSACK: Your Honor, I just have one minor
13   clarification question for the record.
14   JUDGE CHAPPELL: All right.
15   - - - - -
16   REDIRECT EXAMINATION
17   BY MS. LASSACK:
18   Q. Professor Hill, you just testified that the
19   relevant time period was 2005 through 2010. Do you
20   recall that testimony?
21   A. Yes.
22   Q. What month in 2010 did the relevant time period
23   for your opinions end?
24   A. July 2010.
25   MS. LASSACK: Thank you.

325

1   No further questions, Your Honor.
2   JUDGE CHAPPELL: Are you going to continue this,
3   Mr. Sherman, or let it go?
4   MR. SHERMAN: Oh, I'm finished, Your Honor.
5   Thank you, Professor Hill.
6   JUDGE CHAPPELL: Thank you, Dr. Hill. You're
7   excused.
8   Next witness.
9   MR. SHERMAN: Oh, Your Honor?
10   For the record, Your Honor --
11   JUDGE CHAPPELL: Does this require Dr. Hill?
12   MR. SHERMAN: Excuse me?
13   JUDGE CHAPPELL: Does this require Dr. Hill's
14   presence?
15   MR. SHERMAN: No, it does not.
16   THE WITNESS: Okay.
17   JUDGE CHAPPELL: I'm sure she's had enough of
18   this room. We're going to let her go.
19   MR. SHERMAN: We'll try to get her out.
20   Your Honor, I want to pose an objection to
21   Dr. Hill's testimony even being accepted as expert
22   witness testimony pursuant to 3.41(b), 16 CFR section
23   3.43(b) and federal rule of evidence 702 --
24   MS. VANDRUFF: Your Honor, I'm sorry to
25   interrupt, but Ms. Lassack has exited the courtroom.

29 (Pages 322 to 325)

326

1   May I ask that she return to hear this argument, sir?
2   JUDGE CHAPPELL: Sure.
3   MR. SHERMAN: I think that's right.
4   MS. VANDRUFF: I'm sorry.
5   MR. SHERMAN: That's okay.
6   (Discussion off the record.)
7   MS. VANDRUFF: Your Honor, thank you for your
8   indulgence.
9   JUDGE CHAPPELL: So you have an objection to all
10   of the expert testimony of Dr. Hill?
11   MR. SHERMAN: Yes, sir.
12   JUDGE CHAPPELL: And what's your basis?
13   MR. SHERMAN: The basis is that Dr. Hill did
14   not determine based on her education and her knowledge,
15   her experience, her conclusions were not consistent
16   with what the facts in the case were. And the fact
17   that Dr. Hill basically, I think, made conclusions not
18   based on the facts as they exist in this case, the fact
19   that she did not consider certain testimony, the fact
20   that her conclusions were not actually based on
21   scientific, technical or other specialized knowledge,
22   it was simply her opinion with regard to what a data
23   security program should look like.
24   In fact, it was her opinion that a
25   comprehensive information security plan was to be

327

1   formulated from a series of documents and a series of
2   reports which taken together would come up with a
3   definition of what she described as a comprehensive
4   information security plan that -- as well as defense in
5   depth, as well as seven principles associated with it.
6   And there is no scientific basis that if taken
7   together, all of those -- all of those aspects even
8   apply on a case-by-case basis to any organization who
9   is dealing with data security, so with that respect --
10   in that respect, we argue that it lacked the scientific
11   methodology in which to come up with what she describes
12   as a comprehensive information security plan.
13   JUDGE CHAPPELL: Are you opposing this
14   objection?
15   MS. LASSACK: Yes, Your Honor.
16   JUDGE CHAPPELL: You can step over here if that
17   will be easier or you're going to break your back there
18   at that microphone.
19   MS. LASSACK: Your Honor, respondent's motion
20   is baseless. As a threshold matter, respondent has
21   been on notice of Professor Hill's opinions and
22   methodology since her expert report was submitted on
23   March 18 --
24   JUDGE CHAPPELL: Let's get past the procedure
25   and let's get to the substance.

328

1   MS. LASSACK: So the standard for admissibility
2   of expert testimony is that the expert's scientific,
3   technical or other specialized knowledge will assist
4   the trier of fact in understanding issues in this case.
5   I think Professor Hill's qualifications clearly
6   establish that she has specialized knowledge in the
7   field of data security. That information will be
8   helpful to the trier of fact.
9   And I don't think the testimony today and
10   yesterday presents any indication that Professor Hill
11   did not consider the relevant facts of this case. To
12   the contrary. Professor Hill considered extensive
13   record evidence, all of which is listed in Appendix B to
14   her report and much of which was shown on the screen
15   during her direct and cross-examination.
16   JUDGE CHAPPELL: Okay. Thank you.
17   MR. SHERMAN: The only other thing I would add
18   for the court's consideration, Your Honor, is the fact
19   that Professor Hill testified that she really didn't
20   have any experience in the medical field in terms of
21   what was necessary for data security protection for an
22   entity that dealt with protected health information or
23   provided medical services.
24   MS. LASSACK: May I, Your Honor?
25   JUDGE CHAPPELL: Go ahead.

329

1   MS. LASSACK: I do not believe that
2   Professor Hill testified that she had no experience
3   about the protection of medical information. She cited
4   to several resources that set out guidelines for
5   protecting medical information. She has experience
6   researching medical data. And the principles that she
7   applied in this case, I think that she's established
8   that they are well-known principles within the
9   IT industry. That would be helpful to the court in
10   deciding issues in this case.
11   JUDGE CHAPPELL: All right. Thank you.
12   MS. LASSACK: Thank you.
13   JUDGE CHAPPELL: You can have a seat.
14   As I stated earlier, we don't have a jury here,
15   and I'm not going to be misled by an opinion of an
16   expert, a real expert, a so-called expert, a pseudo
17   expert. If I find that I need the assistance of an
18   expert and I find that that expert is qualified to give
19   me an opinion, I will consider that opinion.
20   I can assure you that when I draft the initial
21   decision in this case, my reasoning and reliance upon
22   any expert opinion will be very clear in the event it's
23   needed by the Court of Appeals down the road to
24   determine why I did what I did.
25   I find that your objection, the basis of your

30 (Pages 326 to 329)

330

1   objection and the reasoning goes to the weight, not the
2   admissibility.
3   I'm going to allow the opinion evidence into the
4   record. It does not mean it will be dispositive of any
5   issue in this case. But I'm not going to strike the
6   testimony. I will make the determination whether I
7   think it's reliable, whether I think it's necessary to
8   support any issue in this case.
9   Thank you.
10   So with that, your objection is overruled.
11   MR. SHERMAN: Thank you, Your Honor.
12   MS. LASSACK: Thank you, Your Honor.
13   JUDGE CHAPPELL: Next witness.
14   MS. VANDRUFF: Thank you, Your Honor.
15   Complaint counsel calls Kevin Wilmer.
16   Your Honor, while Mr. Wilmer joins us in the
17   courtroom -- and he's just outside. There will be no
18   delay -- we do have copies of one of two documents that
19   we will use during Mr. Wilmer's examination for
20   Your Honor, for the court reporter, for your law clerk,
21   if that would be helpful.
22   JUDGE CHAPPELL: I don't have a law clerk. I
23   have an attorney advisor. But if we need copies, we'll
24   let you know. Thank you.
25   MS. VANDRUFF: Thank you, Your Honor.

331

1   JUDGE CHAPPELL: Ironsides, you and
2   Officer Proctor are going to get the witness squared
3   away, once he's sworn, with the microphone?
4   - - - - -
5   Whereupon --
6   KEVIN WILMER
7   a witness, called for examination, having been first
8   duly sworn, was examined and testified as follows:
9   MS. VANDRUFF: May I proceed, Your Honor?
10   JUDGE CHAPPELL: Go ahead.
11   - - - - -
12   DIRECT EXAMINATION
13   BY MS. VANDRUFF:
14   Q. Mr. Wilmer, will you please introduce yourself
15   to the court.
16   A. My name is Kevin Wilmer. I'm a Federal Trade
17   investigator for the Bureau of Consumer Protection, the
18   Division of Privacy and Identity Protection.
19   Q. How long have you worked at the
20   Federal Trade Commission?
21   A. This month will mark six years. I began in
22   May of 2008.
23   Q. Describe your employment history prior to
24   becoming an investigator at the
25   Federal Trade Commission.

332

1   A. Prior to coming to the Federal Trade Commission,
2   I was a compliance analyst for the Maryland
3   Board of Physicians. It was previously known as the
4   Board of Physician Quality Assurance. It is a state
5   regulatory agency which licenses and regulates
6   physicians in Maryland as well as investigates
7   disciplinary actions.
8   Q. For how long did you work with the
9   Maryland Board of Physicians as a compliance analyst?
10   A. I worked for the Maryland Board of Physicians as
11   a compliance analyst for approximately 16 years.
12   Q. And where did you work prior to working at the
13   Maryland Board of Physicians?
14   A. Prior to the Board of Physicians, I was a
15   paralegal with the law firm of Piper & Marbury in
16   Baltimore, Maryland.
17   Q. Mr. Wilmer, have you ever served in the
18   United States military?
19   A. Yes, I have.
20   Q. In what branch did you serve, sir?
21   A. I served in the United States Air Force Reserve.
22   Q. During what period did you serve in the
23   Air Force Reserves?
24   A. I honorably served in the Air Force Reserves
25   from February of '82 to June of '94.

333

1   Q. And what was your rank when you separated from
2   service?
3   A. I separated with the rank of staff sergeant.
4   JUDGE CHAPPELL: E4? That was E4?
5   THE WITNESS: I was E5, sir.
6   MS. VANDRUFF: Thank you, Your Honor.
7   BY MS. VANDRUFF:
8   Q. Describe your educational background.
9   A. I have a bachelor's degree from the
10   University of Baltimore in interdisciplinary studies.
11   My areas of concentration were business administration,
12   corporate communications, and philosophy.
13   Q. Have you done any graduate work?
14   A. I attended the University of Baltimore
15   School of Law, and I took a leave of absence after my
16   2L year.
17   Q. I believe you described for His Honor that you
18   work in the Division of Privacy and Identity Protection
19   here at the Federal Trade Commission.
20   Describe the work that you perform for the
21   Division of Privacy and Identity Protection.
22   A. As a Federal Trade investigator, I do a variety
23   of functions in the Division of Privacy and Identity
24   Protection. Primarily we identify -- we investigate
25   matters dealing with identity protection and identity

334

1   theft, but I'm also the liaison for the division to the
2   Maryland financial crimes working group, which is an
3   identity theft working group associated with the
4   U.S. Attorney's Office for the State of Maryland.
5   In addition to that, I also do consumer and
6   business outreach, workshops in matters of identity
7   security and identity theft.
8   Q. When we go into our in camera session -- and
9   Your Honor, I will request that in a few moments -- but
10 when we do that, I will ask you about the work that
11 you've done specifically in this case, Mr. Wilmer.
12   But as a preliminary matter, was your work in
13 this case performed at the direction of counsel?
14   A. Yes.
15   Q. And specifically who asked you to do work in
16 this case?
17   A. You did.
18   Q. So for a moment let's turn back to your work as
19 an investigator.
20   At the Federal Trade Commission, have you
21 received training in investigatory techniques?
22   A. Yes, I have.
23   Q. Are you familiar with the West Thomson Reuters
24 product CLEAR?
25   A. Yes, I am.

335

1   Q. What is CLEAR?
2   A. CLEAR is an investigative tool used by
3   investigators here at the Federal Trade Commission to
4   obtain information on both individuals and
5   corporations.
6   Q. Have you received training regarding the use of
7   CLEAR in investigations?
8   A. Yes, I have.
9   Q. Describe those trainings for the court.
10   A. The initial training consisted of the training
11 provided by the CLEAR representatives, and the
12 continuing training has been continuing education
13 matters that help us to make the job easier.
14   Q. Based on your training and experience,
15 Mr. Wilmer, do you have an understanding of what
16 information regarding individuals is contained in
17 CLEAR?
18   A. Yes, I do.
19   Q. What is your understanding?
20   A. It's my understanding that the information
21 contained in CLEAR is aggregated from a variety of
22 sources: credit bureau information, utility
23 information, all forms of public information, and
24 information from civil judgments to criminal
25 convictions.

336

1   MS. VANDRUFF: At this time, Your Honor, I
2   would respectfully request that we go into an in camera
3   session so that I may conclude my examination of
4   Mr. Wilmer, which will relate to two documents that
5   Your Honor has granted in camera status.
6   JUDGE CHAPPELL: All right. At this time I'm
7   going to be clearing the courtroom of those people that
8   are not subject to the protective order in this case.
9   We're going to go into a closed session.
10   Ironsides, Mr. Proctor, one of you, would you
11 turn the sign, please.
12   And for those of you that are going to exit the
13 courtroom, if you -- I don't know how long this will
14 take, but the sign will be turned and you'll be welcomed
15 in when this closed session is finished.
16   And to make this process easier, I'm going to
17 ask counsel to look behind you and see if you can
18 verify that the people that are behind you that remain
19 are subject to the protective order in this case,
20 meaning they've acknowledged what they need to
21 acknowledge to access the information.
22   Mr. Sherman, just so we're clear, I think -- I
23 don't know about this particular information, but based
24 on some pleadings and rulings I've made, are there some
25 issues with your client as to some of the in camera

337

1   information or is he okay to hear everything?
2   MR. SHERMAN: I believe my client is subject to
3   the protective order, Judge, in that he will not
4   disclose. Now, if the court feels otherwise, then he
5   can be excused. But in terms of what I understand are
6   his rights of confrontation in these situations, I
7   think that I would argue that he should stay and that
8   as a party in this case he has every right to and that
9   he is in fact subject to the protective order.
10   MS. VANDRUFF: And Your Honor, if I may be
11 heard, I know that in competition matters there are
12 sometimes competitively sensitive information that are
13 also subject to in camera orders. That's not the case
14 here, Your Honor, and complaint counsel has no objection
15 to Mr. Daugherty's presence.
16   JUDGE CHAPPELL: Okay. Thank you.
17   MR. SHERMAN: Thank you, Counselor.
18   JUDGE CHAPPELL: We are now in in camera
19 session, and you may continue.
20   (Whereupon, the proceedings were held in
21 in camera session.)
22   - - - - -
23
24
25

32 (Pages 334 to 337)

378

1   C corp.
2   **Q. And can you describe how the company is run.**
3   A. It's run with an executive management team to
4   which I'm a part of running day-to-day operations.
5   **Q. And who reports to the executive team?**
6   A. All of the other functions within the company
7   report to the executive team.
8   **Q. Mr. Kam, what does ID Experts do?**
9   A. They provide data breach services, response
10   services, as well as assistance to victims of identity
11   theft and medical identity theft.
12   **Q. You just testified that the company specializes**
13   **in data breach response.**
14   **What is a data breach, Mr. Kam?**
15   A. A data breach is typically when an organization
16   has an unauthorized disclosure of sensitive personal
17   information and has to respond by notifying consumers
18   and other regulatory bodies.
19   **Q. And so what do you mean by "data breach**
20   **response"?**
21   A. It's the services typically that assist the
22   breaching organization in responding to those consumers,
23   providing consumer notification, and in particular
24   helping those individuals who identify themselves as
25   victims of identity theft or medical identity theft

379

1   recover to pretheft status.
2   **Q. And what types of clients or organizations has**
3   **ID Experts assisted with a breach response?**
4   A. We've helped many of the federal agencies up
5   here on the Hill, as well as state and local
6   organizations, healthcare organizations, financial
7   services organizations, as well as many of the
8   universities around the country.
9   **Q. So when a client of ID Experts' has a breach or**
10   **an unauthorized disclosure, can you please explain to**
11   **Judge Chappell the services that ID Experts might**
12   **provide to that client.**
13   A. It basically falls into three areas, the first
14   being assisting with the risk assessment to determine
15   the possibilities or the likely harms that might befall
16   the people who have been affected by that particular
17   incident.
18   It then involves assisting the organization in
19   the development of an incident response plan, basically
20   a response that provides communications to those
21   individuals.
22   The second area is typically providing the
23   printing of the notification letters, mailing of those
24   letters, as well as provision of call center services so
25   when consumers receive notification, they have a

380

1   consumer hotline to call into to understand what the
2   risk might be based on the information that was
3   disclosed.
4   And third, really where our specialty lies and
5   where we started the company many years ago was really
6   helping people who fall victim to identity crimes
7   identify the issues that have been created by identity
8   thieves and return them to pretheft status.
9   **Q. So why would a company engage an entity like**
10   **ID Experts after an unauthorized disclosure or a**
11   **breach?**
12   A. Typically what will happen, an organization
13   that has a data breach may only experience this
14   particular incident once or twice or a handful of times
15   in the course of the careers of the people that are
16   part of the company, whether it's the executive team or
17   the privacy officer, and so they're looking for
18   experts, essentially an organization to help them
19   through the process, an organization that has been
20   through it many times before so that it can guide the
21   whole process, making sure there's positive outcomes
22   from the event, and most specifically helping those
23   people who have actually fallen victim to identity theft
24   or medical identity theft.
25   **Q. And approximately how many breaches or**

381

1   **unauthorized disclosures has ID Experts worked on since**
2   **the company was founded?**
3   A. We've literally worked on hundreds of events. I
4   would say close to a thousand at this point.
5   **Q. Have you personally worked on any?**
6   A. Yes.
7   **Q. Of those that you have worked on, how would you**
8   **characterize your level of involvement?**
9   A. I typically play two roles. The first is as an
10   executive liaison to either the board or the management
11   team. And the second is, when there is media involved,
12   as the PR representative on behalf of that client.
13   **Q. And why would you serve as an executive**
14   **liaison?**
15   A. Well, what typically happens is that an
16   organization, again, may not have experienced something
17   like this before, a breach of personal -- sensitive
18   personal information, so the executive team wants
19   reassurance that we, as the organization helping them,
20   understand the nature and the risks that they're
21   facing.
22   And more specifically, they want to see us --
23   see me involved in making sure that they receive the
24   attention and all of the services to help them
25   remediate the risks.

374

(lines 4-25, no text)

375

1   (Pause in the proceedings.)
2   JUDGE CHAPPELL: It looks like the fates are
3   against me in not having a break, so we're going to
4   recess. We'll return at 4:00 p.m.
5   We're in recess.
6   (Recess)
7   JUDGE CHAPPELL: All right. Back on the record.
8   Next witness.
9   MS. VANDRUFF: Your Honor, before we call
10   Mr. Kam, can I just deal with one preliminary matter?
11   JUDGE CHAPPELL: All right.
12   MS. VANDRUFF: Your Honor, yesterday I
13   represented that the parties had only served on your
14   office JX 2, which is the parties' stipulation
15   regarding the admissibility of certain exhibits. I was
16   mistaken in that representation. I apologize.
17   We are filing jointly, with respondent's
18   counsel's consent, a motion to withdraw JX 2 that had
19   been submitted last week because Your Honor has
20   admitted the JX 2 that superseded that, and I just
21   wanted to advise Your Honor of my misrepresentation.
22   JUDGE CHAPPELL: Oh, I think I follow you. It
23   was actually a motion or it was actually filed with --
24   MS. VANDRUFF: It was actually filed with the
25   Office of the Secretary. And following Your Honor's

376

1   guidance yesterday, we are at this time filing a motion
2   that's being filed with the Office of the Secretary to
3   withdraw --
4   JUDGE CHAPPELL: It doesn't need to be a
5   motion. Then I have to rule on that. Just a notice of
6   withdrawal, a joint notice of withdrawal. That way, I
7   don't have to rule on it.
8   And so we're clear, the JX 2 in the record is
9   the proper one.
10   MS. VANDRUFF: Yes, Your Honor. There's no
11   dispute about that. Thank you.
12   JUDGE CHAPPELL: All right. Thank you.
13   MR. SHERMAN: That's our understanding,
14   Your Honor.
15   JUDGE CHAPPELL: Okay. Thank you.
16   MR. MEHM: Your Honor, complaint counsel would
17   now like to call Mr. Kam to the stand.
18   And I want to also take this opportunity to
19   apologize for the slight delay about finding Mr. Kam.
20   JUDGE CHAPPELL: Where was he?
21   MR. MEHM: I think he may have just gone to
22   the -- I don't know. I think -- we found him. He is
23   here.
24   JUDGE CHAPPELL: You felt better after he showed
25   up; right?

377

1   - - - - -
2   Whereupon --
3   RICHARD LAWRENCE KAM
4   a witness, called for examination, having been first
5   duly sworn, was examined and testified as follows:
6   DIRECT EXAMINATION
7   BY MR. MEHM:
8   Q. Good afternoon, Mr. Kam.
9   Please introduce yourself to the court.
10   A. My name is Richard Lawrence Kam, spelled K-A-M.
11   Q. And where are you currently employed?
12   A. At a company called ID Experts.
13   Q. And what is your title?
14   A. I'm the president and cofounder of ID Experts.
15   Q. And where is ID Experts based?
16   A. It's based in Portland, Oregon.
17   Q. And how many people does ID Experts currently
18   employ?
19   A. We have 53 full-time equivalents.
20   Q. When did you found the company?
21   A. I founded the company back in 2003.
22   Q. How long have you worked at ID Experts?
23   A. Since that time.
24   Q. And how is the company structured?
25   A. It's structured as a C corp., traditional

42 (Pages 374 to 377)

382

1   Q. So when you serve as executive liaison, how
2 often might you typically interact with the executive
3 team that you just referred to?
4   A. When the organization first engages us,
5 typically I'm involved in the very beginning,
6 describing the services that we can provide, helping
7 them assess the potential risks that they may face.
8 And then as we engage, it typically is in many cases on
9 a daily basis for several weeks.
10   Q. Now, you stated earlier that ID Experts also
11 specializes in assisting victims of identity theft and
12 medical identity theft.
13   What did you mean by that?
14   A. When someone falls victim to identity theft,
15 there are a lot of issues that occur that the identity
16 thieves create, and so we've developed a business that
17 under limited power of attorney provides recovery
18 advocacy, recovery advocates, people who are
19 specialists in helping a victim identify the issues
20 that have been created by an identity thief and work
21 with them to expunge all of the negative records from
22 their accounts.
23   Q. Have you worked with victims of identity theft?
24   A. Yes.
25   Q. Describe the work that you've performed with

383

1 victims of identity theft.
2   A. So as recently as a couple of days ago,
3 essentially what will happen is people who I know or
4 know me will reach out and ask for assistance. They
5 will typically do that because they're looking for
6 someone who is empathetic, understands the issues of
7 identity theft, someone who they can look to who is an
8 expert in the issue and someone who will take care of
9 their problems, so I'll get involved with typically
10 more significant forms of identity theft and medical
11 identity theft.
12   And essentially once I kind of help them
13 understand what the potential issues are and the fact
14 that they may have actually fallen victim to identity
15 theft and medical identity theft, I'll assign somebody
16 from my team who will then again work under limited
17 power of attorney to identify all of the issues the
18 victim may have seen and help them return to pretheft
19 status.
20   Q. And can you describe ID Experts work with
21 victims of medical identity theft.
22   A. Well, like victims of identity theft, medical
23 identity theft, unfortunately, is more complex, and so
24 it takes someone who is versed in some of the issues
25 that a medical identity theft victim will see and

384

1 specifically working with the institutions where this
2 situation will crop up, like hospitals, payers and
3 others, to be able to work them through, work with them
4 to identify those issues and resolve them.
5   Q. Can you please provide Judge Chappell with a few
6 examples of the types of identity theft or medical
7 identity theft cases that you or the teams working under
8 your supervision have helped resolve.
9   A. Well, it really ranges from an identity theft
10 victim whose information may be used to get access to
11 their existing accounts, perhaps a checking or savings
12 account.
13   It may be a situation where an identity theft
14 victim may have a -- their identity used to get tax
15 refunds on the behalf of the identity thief, thereby
16 delaying the ability for the victim to essentially get
17 access to their -- or file their taxes and get access to
18 their returns.
19   In the case of medical identity theft
20 specifically, there have been cases that we've worked
21 on where the electronic health file, the medical
22 record, if you will, of the victim has been
23 compromised, and we've had to work with not only the
24 victim but the hospital, the payers, the labs, the
25 organizations where this information has been corrupted

385

1 essentially to identify that this individual is a victim
2 of medical identity theft and help them return to
3 pretheft status.
4   Q. In order to fully understand identity theft and
5 medical identity theft and its consequences, how
6 important is it to have practical experience like
7 yours?
8   A. You know, I think it's extremely important.
9   Again, I mentioned the aspect of trust. People
10 who fall victim to identity theft and, unfortunately,
11 medical identity theft feel like victims of spouse
12 abuse, as an example. They're embarrassed. In many
13 cases, they feel they may have let this happen to them
14 themselves.
15   And so they're looking for people who are
16 empathetic, who will listen and then demonstrate an
17 ability to help them recover to pretheft status.
18   Q. And how has having over a decade of
19 on-the-ground daily experience with identity theft and
20 medical identity theft helped you understand these
21 issues?
22   A. You know, it's given me a very unique
23 perspective. You know, until you actually go through
24 it, if you have never fallen victim to identity theft
25 or have talked to somebody who has, you really don't

386

1   have a view of what happens and how people feel about
2   this.
3   And so, you know, literally working with the
4   hundreds in my case and in the case of my team tens of
5   thousands of individual victims has given me true
6   empathy for these people and what they're going through
7   and, unfortunately, all of the horrible experiences that
8   occur when they fall victim to identity theft and
9   medical identity theft.
10   Q. And setting aside for right now your experience
11   with ID Experts, in what other ways have you worked on
12   privacy issues, including identity theft or medical
13   identity theft?
14   A. I've had the opportunity over the years to
15   participate in several data privacy working groups
16   where we've not only identified some of the key issues
17   around identity theft, medical identity theft and data
18   breach but also have had the opportunity to publish
19   white papers that help educate consumers as well as
20   legislators and other -- and business about this
21   particular topic.
22   Q. And what working groups in these areas are you
23   currently a member of?
24   A. There's a list of them. I'll just quickly list
25   them.

387

1   They include the International Association of
2   Privacy Professionals, IAPP.
3   It includes the Health Care Compliance
4   Association, HCCA.
5   It includes the Health Information Management
6   Systems Society, HIMSS.
7   And the Medical Identity Fraud Alliance, MIFA
8   for short.
9   Q. So I'd like to take a moment and very quickly
10   focus on your work with MIFA.
11   What is the Medical Identity Fraud Alliance?
12   A. The Medical Identity Fraud Alliance is an
13   alliance of approximately forty organizations that was
14   put in place as of October of 2013.
15   Q. And what is the goal of MIFA?
16   A. The goal of MIFA is to bring together these
17   organizations and essentially to help identify best
18   practices in the fight against medical identity theft
19   and medical fraud.
20   Q. And how does MIFA --
21   JUDGE CHAPPELL: Excuse me.
22   Is an organization that didn't start until
23   October 2013 relevant to this case?
24   BY MR. MEHM:
25   Q. Well, can you describe, Mr. Kam, for

388

1   Judge Chappell when that -- that was when my
2   understanding is the group was officially formed,
3   but --
4   A. Right.
5   Q. -- there was some work that was done before
6   that. It might help, Mr. Kam, if you explain to
7   Judge Chappell the work that was done prior to the
8   official formation of MIFA.
9   A. You know, prior to October '13, Your Honor, the
10   idea of the Medical Identity Fraud Alliance actually
11   came up late 2012. And the idea stemmed from the work
12   that was done by an organization called the
13   Financial Services Roundtable, literally the hundred
14   largest banks in the U.S. getting together to develop
15   best practices in the fight against financial fraud.
16   So several of us in the industry decided that
17   we wanted to see if it was applicable to transfer the
18   knowledge that we all had from the financial services
19   industry in fighting financial fraud and identity theft
20   to the healthcare industry, and so on March -- or in
21   March of 2013, 40 of us -- 35 to 40 of us got together
22   in Boston, and we decided that engaging the consumer in
23   the fight against medical identity theft and medical
24   fraud was something that needed to happen in the
25   healthcare industry.

389

1   And therefore, organizations today like
2   UnitedHealthcare, Aetna, Kaiser Permanente, AARP,
3   Blue Cross Blue Shield Association, the National Health
4   Care Anti-Fraud Association, and many others have joined
5   forces essentially to provide resources to identify the
6   problem and to educate the consumer.
7   Q. And beyond the work that you did in founding
8   MIFA, can you tell Judge Chappell just a little bit more
9   about your work with this group.
10   MS. MORGAN: Your Honor, I object to further
11   testimony on MIFA, and I ask that the testimony on MIFA
12   be stricken on the grounds that it is not relevant to
13   this case because it was founded in 2012 and did not
14   begin working until 2013.
15   MR. MEHM: Your Honor, the reason that we are
16   just very briefly eliciting some testimony on this
17   illustrative example of one of the working groups that
18   Mr. Kam testified that he's involved with is to provide
19   the court with some flavor of his background, his
20   experience in working with identity theft and medical
21   identity theft since that bears directly on the
22   testimony and his opinions in this case and the facts of
23   this case.
24   JUDGE CHAPPELL: Well, based on the objection,
25   I'm not going to strike it or disregard it, but I get

45 (Pages 386 to 389)

390

1   the gist of it, so let's summarize and move on and get
2   to the opinions.
3   MR. MEHM: Absolutely, Your Honor.
4   JUDGE CHAPPELL: So the objection is overruled,
5   I guess in part overruled.
6   MR. MEHM: Your Honor, with the court's
7   indulgence, may I ask Mr. Kam just a handful, very small
8   handful, a few more questions --
9   JUDGE CHAPPELL: Go ahead. But we're getting
10   too much into the weeds here on something.
11   MR. MEHM: Gotcha. I got it, Your Honor.
12   Thank you.
13   BY MR. MEHM:
14   Q. So, Mr. Kam, what professional boards or
15   organizations have you belonged to in the past that
16   relate to privacy, including identity theft or medical
17   identity theft?
18   A. You know, I've worked on several working groups
19   that include the International -- ANSI,
20   American National Standards Institute, the
21   Internet Security Alliance, and The Santa Fe Group
22   Shared Assessments Program.
23   Q. Were you invited to participate in any of the
24   working groups that you just testified about?
25   A. Yes.

391

1   Q. Which ones?
2   A. Specifically with the American National
3   Standards Institute's projects.
4   Q. Are you invited to speak or present regularly on
5   identity theft and medical identity theft?
6   A. Yes.
7   Q. What types of conferences or meetings have you
8   presented at?
9   A. You know, I've presented at meetings of the
10   International Association of Privacy Professionals over
11   the years, the Health Care Compliance Association, as
12   well as the health information management HIMSS
13   organization that I mentioned earlier.
14   Most recently it's been even with the
15   American Bar Association. I'm presenting next month to
16   15,000 attorneys across the U.S. on this particular
17   topic.
18   Q. And how often, approximately, do you speak on
19   identity theft, medical identity theft or privacy
20   issues?
21   A. It's probably once or twice a month.
22   Q. And have you published articles or other pieces
23   on medical identity theft and identity theft?
24   A. Yes.
25   Q. And where have some of those articles or other

392

1   pieces been published?
2   A. You know, they'll show up -- I have a monthly
3   column that Government Health IT asked me to write, as
4   well as it will show up in media like Bloomberg,
5   CBSNews.com, Forbes, other, other publications.
6   Q. And approximately how many of these articles
7   have been published?
8   MS. MORGAN: Objection, Your Honor.
9   Questions regarding the publication of news
10   articles in publications such as Bloomberg are not
11   relevant to this expert's -- or to this witness'
12   expertise.
13   JUDGE CHAPPELL: Are they in his CV?
14   MR. MEHM: I'm sorry, Your Honor. I couldn't
15   hear.
16   JUDGE CHAPPELL: Are these publications listed
17   in his CV that should be in the record?
18   MR. MEHM: Mr. Kam?
19   THE WITNESS: Yes, they are.
20   JUDGE CHAPPELL: Then we don't need to hear this
21   information.
22   That objection is sustained.
23   We don't need to repeat here what's already in
24   the record.
25   MR. MEHM: Understood.

393

1   JUDGE CHAPPELL: I don't think you were here
2   earlier.
3   MR. MEHM: I'm sorry, Your Honor?
4   JUDGE CHAPPELL: I don't think you were here
5   earlier when the previous expert --
6   MR. MEHM: I was not here earlier today, so I
7   apologize if I missed that instruction.
8   BY MR. MEHM:
9   Q. What professional certifications, if any, do you
10   hold, Mr. Kam?
11   A. I hold a certification CIPP, a
12   Certified Information Privacy Professional
13   certification.
14   Q. And how long have you held that certification?
15   A. Since April 2010.
16   MR. MEHM: Your Honor, pursuant to commission
17   rule 3.31(a), I am tendering Mr. Kam as a qualified
18   expert witness in the field of medical identity theft
19   and identity theft.
20   MS. MORGAN: I object, Your Honor.
21   JUDGE CHAPPELL: On what basis?
22   MS. MORGAN: On the grounds that his expertise
23   has not been established, nor has his methodology been
24   tested, nor has his expertise specifically as pertains
25   to this case been established.

46 (Pages 390 to 393)

394

1   JUDGE CHAPPELL: The objection is overruled.
2   And you don't have to formally tender an expert
3 in these proceedings. To the extent any opinions meet
4 the proper legal standards, they'll be considered.
5   Go ahead.
6   BY MR. MEHM:
7   **Q. Mr. Kam, when a company or other organization**
8 **experiences an unauthorized disclosure involving**
9 **sensitive consumer information, what types of harms can**
10 **a consumer whose information was disclosed suffer?**
11   A. It falls in a couple of areas, one being
12 identity theft and the other being medical identity
13 theft.
14   **Q. And what, Mr. Kam, is identity theft?**
15   A. Identity theft is when somebody uses another
16 person's identity without their permission. It
17 includes specifically things like their name, date of
18 birth, Social Security number, and perhaps financial
19 information to commit various identity theft crimes.
20   **Q. And can you describe what type of harms or**
21 **injuries do identity theft victims typically suffer.**
22   A. It falls in a couple of areas, one being
23 financial harms. Essentially an identity thief could
24 take over a victim's existing checking account, savings
25 account, perhaps their brokerage account.

395

1   An identity thief may set up new accounts on the
2 victim's behalf, which might include credit accounts,
3 credit cards, gift cards, and so forth.
4   They may try to use that individual's identity
5 to impersonate or mask their own identity if they have a
6 criminal record or may have other issues with their own
7 identity.
8   And in the case of medical identity theft, there
9 are other harms that might occur.
10   **Q. And why would someone use another person's**
11 **identity without his or her permission?**
12   A. It's typically to -- for illicit financial
13 gain.
14   **Q. And what, Mr. Kam, is medical identity theft?**
15   A. Medical identity theft is when another person
16 uses someone's medical identity and to get access to
17 goods, services, prescription drugs perhaps, or to
18 fraudulently bill private public insurance like Medicare
19 and Medicaid.
20   **Q. And can you describe some of the harms that a**
21 **victim of medical identity theft -- excuse me. Strike**
22 **that.**
23   **Can you please describe some of the harms that a**
24 **victim of medical identity theft may experience.**
25   A. A victim of medical identity theft will

396

1 experience financial, reputational and other harms.
2   **Q. And what types of information are frequently**
3 **used to commit medical identity theft?**
4   A. It includes name, date of birth, Social Security
5 number, health insurance number, as well as health
6 history and health information.
7   **Q. And how difficult is it for a consumer whose**
8 **information was disclosed in an unauthorized disclosure**
9 **to detect that he or she has become a victim of medical**
10 **identity theft?**
11   A. It's very difficult to detect.
12   **Q. And how about identity theft?**
13   A. Very difficult to detect.
14   **Q. Is it possible for a consumer to always know**
15 **about the security practices of every company that**
16 **collects or maintains his or her personal information?**
17   MS. MORGAN: Objection, Your Honor. This is
18 outside the scope of the expert report that was provided
19 to respondents.
20   MR. MEHM: Your Honor, if I may, this
21 information is directly in Mr. Kam's report.
22   JUDGE CHAPPELL: Well, when we have an objection
23 that an opinion is not in the report, you'll need to lay
24 the foundation with the witness to demonstrate where it
25 is in the report.

397

1   MR. MEHM: Okay. So we will.
2   JUDGE CHAPPELL: At this time I won't rule on
3 the objection. You'll have an opportunity to
4 demonstrate that this opinion is in the report and where
5 it is.
6   MR. MEHM: And we absolutely will. Thank you,
7 Your Honor.
8   BY MR. MEHM:
9   **Q. Mr. Kam, can you please take a look at your**
10 **report that has been premarked as CX 0742. Your report**
11 **should be in the binder that is close to your chair.**
12   A. I'm sorry. Did you say CX 0742?
13   I see it. Thank you.
14   **Q. Yes. There is a tab in the binder that's**
15 **labeled CX 0742.**
16   **Do you recognize this document?**
17   **(Pause in the proceedings.)**
18   A. Yes, I do.
19   **Q. What is it?**
20   A. It's my expert report on the LabMD matter.
21   **Q. Who drafted this document?**
22   JUDGE CHAPPELL: You don't need to lay a
23 foundation for the report. It's already in evidence.
24 You need to demonstrate that the question you asked the
25 witness is in his report. That was the objection.

47 (Pages 394 to 397)

                                                                                                    398

1   BY MR. MEHM:
2   Q. Could you please turn, Mr. Kam, to page 17 of
3   your report.
4   And could you please look under the heading that
5   is approximately half bay down the page entitled
6   Consumers' Ability to Avoid Possible Harms.
7   A. Yes. I'm there.
8   Q. Could I direct you, Mr. Kam, please, to the
9   first sentence of that paragraph.
10   A. Uh-huh.
11   Q. And so in light of that, let me ask you again,
12   is it possible for a consumer to always know about the
13   security practices of every company that collects or
14   maintains his or her personal information?
15   A. As I expressed in my report, a consumer cannot
16   know about the security practices of every company that
17   collects or maintains his or her personal information.
18   JUDGE CHAPPELL: And seeing that in the report,
19   my ruling on the objection is, shall we say, touché.
20   Overruled.
21   BY MR. MEHM:
22   Q. Is it always possible, Mr. Kam, for a consumer
23   to connect the dots by identifying the source of the
24   information used to harm them?
25   A. No. It's very difficult actually.

                                                                                                    399

1   Q. Why?
2   A. In the case of identity theft, again, a consumer
3   may not know who -- which companies have their
4   information.
5   In the case of medical identity theft, an
6   electronic health record or a paper-based medical
7   record is distributed among many of the participants in
8   the healthcare ecosystem, so one instance of a
9   healthcare record perhaps at a doctor's office may also
10   appear at several other organizations, including the
11   person's health insurance company. It may be at the
12   medical laboratory of that -- that the -- that that
13   provider works with. It may be in dozens of other
14   instances.
15   Q. Looking again at page 17 of your report under
16   that same heading --
17   JUDGE CHAPPELL: Let me be clear. I don't want
18   to throw you off your game here. You don't have to
19   track the report. Just don't elicit opinions from the
20   expert that aren't in his report.
21   MR. MEHM: I'm sorry, Your Honor. I'm having a
22   little trouble hearing you.
23   JUDGE CHAPPELL: Does anyone else hear me?
24   MR. SHERMAN: I can hear you, Judge.
25   JUDGE CHAPPELL: I'm saying, you don't have to

                                                                                                    400

1   track the report in your question. Just don't ask for
2   opinions to be elicited from the witness that are not in
3   the expert report.
4   I feel like since the objection you feel like
5   you have to go word by word through the report. You
6   don't have to do that. But just don't ask him to form
7   an opinion that's not contained in the report that was
8   submitted prior to trial.
9   MR. MEHM: I understand. Thank you.
10   BY MR. MEHM:
11   Q. On page 17 of your report, Mr. Kam, can you talk
12   about the role, just very briefly, looking at those
13   couple paragraphs there, the role that notification
14   plays in consumers' ability to avoid potential harms
15   from identity theft and medical identity theft.
16   A. Yes.
17   So because of the difficulty a consumer has in
18   knowing when an organization has disclosed the
19   information or had some kind of an issue relative to a
20   security failure, 41 states actually have put in place
21   data breach notification laws to compel organizations
22   to notify consumers of not only when a breach may have
23   occurred but also the types of information that have
24   been disclosed so that the consumer has the opportunity
25   to reduce their risk to falling victim to identity theft

                                                                                                    401

1   or medical identity theft.
2   Q. And without notification, would consumers have
3   any way of independently knowing about an
4   organization's unauthorized disclosure of their
5   sensitive information?
6   A. As I stated in my report, consumers would have
7   no way of knowing independently about an organization's
8   unauthorized disclosure of their sensitive personal
9   information.
10   Q. Does notification, however, eliminate the risk
11   of harm to consumers from identity theft or medical
12   identity theft?
13   A. You know, unfortunately not.
14   Consumers, even if notified by receiving a
15   first-class letter in the mail perhaps or receiving an
16   e-mail, often don't take the actions necessary to
17   reduce their risk of identity theft or medical identity
18   theft.
19   And in fact, many of the studies that have been
20   done over the last couple of years have shown that
21   consumers who are notified that their information has
22   been disclosed in the breach are actually at an
23   elevated risk of falling victim to various identity
24   crimes.
25   Q. And how does the fact that a consumer's

                                                                                48 (Pages 398 to 401)

402

1   sensitive personal information was disclosed increase
2   the risk of harm to them?
3   A. Primarily because their information is now out
4   and available with the consumer having little if not any
5   control over who may access that information.
6   Q. Let me turn back to your report. You testified
7   about it just a moment ago, and I asked you some
8   preliminary questions about it.
9   What did the FTC staff ask you to do in
10   preparing this report?
11   A. The FTC asked me to assess the likely risk of
12   injury, particularly from medical identity theft, to
13   consumers whose information was disclosed in an
14   unauthorized disclosure.
15   Q. And so in your report, you use the terms both
16   "injury" and "harm."
17   In your report and in your testimony here today,
18   do those terms mean the same thing?
19   A. Yes. I use "injury" and "harm" synonymously.
20   Q. And what did you rely upon in preparing your
21   report?
22   A. You know, I relied on several things.
23   The documents that were provided by the
24   Federal Trade Commission.
25   My experience over the last 11 years working

403

1   with victims of identity theft and medical identity
2   theft, as well as clients who have breached sensitive
3   personal information.
4   And also a literature review of what I believed
5   was the most relevant research and information specific
6   to identity theft, medical identity theft and data
7   breach.
8   Q. And Mr. Kam, what is your opinion about the risk
9   of harm to consumers from LabMD's failure to provide
10   reasonable and appropriate security for sensitive
11   personal information?
12   A. It's my opinion that there is a significant risk
13   of injury, risk of harm, a substantive risk of harm, to
14   these individuals from the unauthorized disclosures made
15   by LabMD.
16   And can I just add one more comment there?
17   Q. Yes.
18   A. I'd just like to clarify for Your Honor, I used
19   the word -- let's see -- in my report --
20   Q. And can you be specific about what page you're
21   looking at, Mr. Kam?
22   A. Yeah.
23   In my report on page 9, I used the word
24   "substantial injury." Again, I'm using probably several
25   words to indicate that level of risk, substantial risk

404

1   of injury.
2   Q. So just to be clear for the record, could you
3   read out the first sentence on page 9 about what your
4   opinion is.
5   A. Yeah.
6   "In my opinion, LabMD's failure to provide
7   reasonable and appropriate security for sensitive
8   personal information, including medical information, is
9   likely to cause substantial injury to consumers and puts
10   them at significant risk of identity crimes."
11   Q. In reaching that conclusion, Mr. Kam, did you
12   consider any specific incidents?
13   A. I considered two incidents, specifically what I
14   identify as the P2P incident in my report as well as the
15   Sacramento incident.
16   Q. And setting aside these two incidents, what else
17   did you look at?
18   A. I also considered LabMD's failure to provide
19   reasonable and appropriate security to put the
20   approximately 750,000 consumers whose information they
21   have on their network at risk of disclosure.
22   Q. Can you please describe your methodology for
23   analyzing the risk of harm from what you term in your
24   report as the P2P disclosure, the Sacramento disclosure,
25   and LabMD's failure to provide reasonable and

405

1   appropriate security for the over 750,000 consumers
2   whose personal information LabMD maintained on its
3   computer networks.
4   A. I use an approach that has two steps
5   essentially, starting with assessing the risk of harm or
6   risk of injury to consumers from identity theft or
7   medical identity theft, which is a four-factor risk
8   assessment.
9   I then go on to look at the amount and the
10   frequency or the impact from the particular facts of
11   the case relative -- in this case relative to the LabMD
12   case to identify what harms might befall these
13   consumers.
14   Q. You just testified that you used four factors to
15   assess -- to assess -- excuse me -- the risk of harm to
16   consumers.
17   What are those four factors?
18   A. It starts with looking at the nature and the
19   extent of the information that was disclosed.
20   Specifically I'm looking for sensitive data elements
21   that include name, date of birth, full nine-digit
22   Social Security numbers, health insurance numbers,
23   medical records that indicate sensitive health --
24   sensitive health issues a patient may have, a consumer
25   may have. I'm looking to identify the number of records

49 (Pages 402 to 405)

406

1   that were disclosed also.
2   So that's the first factor.
3   Q. Can you please go on to describe briefly the
4   other three factors.
5   A. Yeah. The other three factors include the --
6   to whom the disclosure was made, was this another
7   employee perhaps, was the disclosure made to another
8   employee, perhaps in the same institution, or was it
9   disclosed the another consumer perhaps or even an
10   identity thief.
11   The third is, was this information accessed and
12   viewed by these individuals.
13   And the fourth is what risk mitigation is taking
14   place in order to reduce the risk of harm to these
15   consumers.
16   Q. And what are these four factors derived from?
17   A. Primarily from my experience working with
18   other -- our clients, as well as working with other
19   privacy professionals who deal with data breaches,
20   you know, within their own organizations.
21   Q. And anything else?
22   A. You know, there may be some specific guides
23   that have been published by various organizations over
24   the last several years.
25   The issue of risk of harm is so central to the

407

1   analysis and the planning once a disclosure is made,
2   it -- it's -- it's central to all discussions that we as
3   privacy professionals have when we're trying to
4   determine what will happen or what could happen to
5   individuals once their unauthorized -- or once their
6   sensitive personal information is disclosed.
7   Q. And why did you use this approach, Mr. Kam?
8   A. When the FTC asked me to do an analysis, I
9   wanted to be sure that others in my profession who
10   could be asked to do something similar would arrive at
11   a similar assessment of risk. And therefore, I looked
12   at a way to make it simple or simpler to understand
13   what is a relatively complex and subjective assessment,
14   and therefore, I used four factors to describe this in
15   my report.
16   Q. Mr. Kam -- excuse me. Court's indulgence.
17   (Pause in the proceedings.)
18   Is part of the reason, Mr. Kam, that you used
19   this methodology or approach so that others could test
20   your method?
21   A. Yes.
22   Q. Mr. Kam, I'd like to ask you some questions now
23   about the exposure of the 1718 File that you refer to in
24   your report as the P2P disclosure.
25   What is the 1718 File?

408

1   A. It's a file indicated by the name that I
2   received called the insurance aging file and includes
3   the sensitive personal information of approximately
4   9300 consumers.
5   Q. And who did this file belong to?
6   A. According to the information I received and
7   reviewed, it belonged to LabMD.
8   Q. And where, where was the 1718 File found?
9   A. According to Robert Boback's testimony, it was
10   first found on February 5, 2008 by his company,
11   Tiversa.
12   Q. And where did Tiversa find the file in
13   February of 2008?
14   A. Again, according to Robert Boback's testimony,
15   it was found on a peer-to-peer network.
16   Q. Was the file found after that?
17   A. Yes.
18   Q. How many times after February 2008 was the file
19   found?
20   A. It was found several times.
21   It was found on November 5, 2008.
22   It was again found on April 7, 2011.
23   It was again found on June 9, 2011 and yet
24   again just before Robert Boback testified in
25   November 2013.

409

1   Q. In what format was the 1718 File discovered?
2   A. It was discovered in clear text, meaning anyone
3   who had access to a peer-to-peer network could view this
4   information.
5   Q. What else was found at the locations where the
6   1718 File was found?
7   A. Robert Boback in his testimony also stated that
8   there was information that could be used to commit
9   identity theft --
10   JUDGE CHAPPELL: I have a question here. Excuse
11   me, Mr. Kam.
12   THE WITNESS: Yes, sir.
13   JUDGE CHAPPELL: Are you asking this witness to
14   insert facts into the record or are you asking him this
15   because this is what he based his opinion on? Because
16   his factual assertions here are not going to have any
17   merit in the record.
18   MR. MEHM: I'm asking these questions,
19   Your Honor, because they are central to the methodology
20   that Mr. Kam used, which we are going to move to very
21   shortly, to discuss his analysis of the risk of harm
22   from this particular instance, so these facts are
23   critical, as Mr. Kam will testify about momentarily, to
24   his analysis.
25   JUDGE CHAPPELL: So if I understand this, he

410

1   based a lot of his opinions on Mr. Boback's testimony.
2   BY MR. MEHM:
3   **Q. Mr. Kam, could you address that.**
4   A. Yes. Yes, sir.
5   So for the P2P incident specifically, the answer
6   is yes.
7   JUDGE CHAPPELL: All right. Thank you.
8   BY MR. MEHM:
9   **Q. And I'm sorry. Let me just look here at the**
10   **screen.**
11   **Mr. Kam, did you get a chance to respond to --**
12   **just -- excuse me. Court's indulgence.**
13   **(Pause in the proceedings.)**
14   **In your experience, Mr. Kam, do identity thieves**
15   **or medical identity thieves look for information on**
16   **peer-to-peer networks?**
17   A. Yes.
18   **Q. And what is your overall assessment of the risk**
19   **of harm to consumers based on the exposure of their**
20   **information in the 1718 File?**
21   A. My overall opinion is they are at significant
22   risk of harm to identity theft and medical identity
23   theft from the unauthorized disclosure of their
24   sensitive personal information.
25   **Q. And how did you conclude this?**

411

1   A. Using the four factors that we described or
2   that we touched on earlier, as well as the other
3   documents that the Federal Trade Commission provided.
4   **Q. And so let's turn now to those factors.**
5   **In applying the first factor, which you**
6   **testified a few moments ago encompasses the nature and**
7   **the extent of the information disclosed, what type of**
8   **information about consumers is contained in the**
9   **1718 File?**
10   A. Specifically in the 1718 File what I reviewed
11   included names, full name, first name, last name, middle
12   initial. It included dates of birth. It included full
13   nine-digit Social Security numbers. It included medical
14   diagnostic codes, CPT codes specifically, as well as
15   billing information and amounts.
16   Oh, and I should mention health insurance
17   numbers, health insurance addresses, health insurance
18   phone numbers and their addresses.
19   **Q. And how would you characterize generally the**
20   **sensitivity of this data?**
21   A. Generally it's very sensitive data. It could be
22   used to commit identity theft and medical identity
23   theft.
24   **Q. And why could this information be valuable to an**
25   **ID thief or a medical ID thief?**

412

1   A. It could be used to commit all -- many forms of
2   identity crimes, both for financial illicit gain as well
3   as to potentially cause embarrassment or for
4   reputational harm.
5   JUDGE CHAPPELL: Is medical ID theft
6   fraudulently procuring someone else's medical benefits?
7   THE WITNESS: Yes. Yes, sir.
8   BY MR. MEHM:
9   **Q. To what extent, Mr. Kam, does a consumer**
10   **generally change any of the information -- and I'm**
11   **talking about the sensitive consumer information -- that**
12   **was exposed in the 1718 File?**
13   A. You know, generally the information in that
14   particular file won't change. There will be
15   circumstances where an individual will change their
16   name. They'll change perhaps their insurance provider,
17   you know, but -- they may even change their address
18   multiple times moving from one place to another. But
19   the -- specifically the Social Security number and their
20   medical history won't change.
21   **Q. And does any of this information have a long**
22   **shelf life or live on for an extended period of time?**
23   A. Yes.
24   Specifically, Ryan, in the case of
25   Social Security numbers, unfortunately, research has

413

1   shown that identity thieves, if they don't use the
2   information themselves, will sell that data to an
3   average of eight other criminals.
4   In the case of health information, specifically
5   health insurance numbers, that information has a very
6   high street value in the black market, so whereas a
7   Social Security number or a credit card payment --
8   credit card number may be worth a dollar in the black
9   market, it's been shown or it's -- you'll see articles
10   reference health information may be worth $50 and
11   upwards of $500 to $1,000 on the black market.
12   **Q. Beyond what you just testified about a**
13   **Social Security number having a long shelf life, is**
14   **there any other categories of data that was contained in**
15   **the 1718 File that typically has a fairly long shelf**
16   **life?**
17   A. Well, essentially the consumer's health record,
18   their health information. If you're diagnosed with
19   prostate cancer or HIV or herpes or hepatitis, that
20   typically doesn't change.
21   **Q. Because some of this data has a long shelf life**
22   **and consumers rarely change it, can you describe how**
23   **consumers are at an ongoing risk of harm from the**
24   **disclosure of that information?**
25   A. Well, from the -- from identity theft, thieves

51 (Pages 410 to 413)

414

1   will continue to or will use that information to commit
2   identity crimes, whether it's, like I mentioned earlier,
3   setting up new accounts or using that person's
4   information for illicit financial gain.
5   In the case of health insurance information,
6   like Your Honor mentioned earlier, use of that
7   information -- or asked earlier about, use of that
8   information to defraud Medicare or Medicaid is a very
9   significant problem today to the tune of anywhere from
10   80 to 120 billion dollars is being defrauded out of the
11   Medicare and Medicaid systems today because of medical
12   identity fraud.
13   Q. And why is it that consumers are at an ongoing
14   risk of harm from the exposure of this information that
15   has a long shelf life and that consumers rarely change?
16   A. It's because this information is out and
17   available and it's impossible to make this information
18   private again, especially the health information.
19   MR. MEHM: Your Honor, I would request --
20   respectfully request that we go into an in camera
21   session at the end of Mr. Kam's examination to discuss
22   the 1718 File, which is CX 0010, which Your Honor
23   previously granted in camera status for.
24   In the in camera session, I also plan, with your
25   permission, to ask Mr. Kam about another document,

415

1   CX 0085, which you also previously granted in camera
2   status for.
3   JUDGE CHAPPELL: Okay. Just to clarify, are you
4   asking for in camera now or are you giving me an
5   advisory warning?
6   MR. MEHM: A heads-up.
7   JUDGE CHAPPELL: So not at this time.
8   MR. MEHM: Not at this time.
9   JUDGE CHAPPELL: Okay. And for future
10   reference, you don't have to tell me what the documents
11   are. I will trust you to know what's in camera. Just
12   ask me for the in camera session.
13   So we're not there yet.
14   MR. MEHM: That's correct, Your Honor.
15   JUDGE CHAPPELL: All right. Let me know.
16   MR. MEHM: Okay. I will. Thank you.
17   BY MR. MEHM:
18   Q. Mr. Kam, let's turn now to the second and third
19   risk factors.
20   In assessing those factors -- and you testified
21   earlier that is to whom the disclosure was made and
22   whether the information was acquired and viewed -- what
23   information did you consider?
24   A. You know, I considered, again, the testimony
25   from Robert Boback, where he stated that that

416

1   information was found -- the information in the
2   1718 File specifically was found at four IP addresses.
3   Q. And were there other elements that you
4   considered from Mr. Boback's testimony regarding the
5   second and third factors?
6   A. Yes. It had -- there was I believe at one of
7   those four IP addresses a suspect who was arrested by
8   federal law enforcement who was suspected of committing
9   identity theft.
10   MS. MORGAN: Objection, Your Honor.
11   JUDGE CHAPPELL: Basis?
12   MS. MORGAN: The witness does not have personal
13   knowledge of this incident. He doesn't know -- he
14   doesn't have personal knowledge of whether anyone was
15   arrested in connection with an IP address.
16   MR. MEHM: Your Honor, Mr. Kam testified that he
17   based his assessment of this -- of these two risk
18   factors on Mr. Boback's testimony and there is
19   information to that effect in the transcript of
20   Mr. Boback.
21   JUDGE CHAPPELL: Well, the way I read this, he
22   was asked what other elements he considered. He told us
23   something he believed. I would think that would be
24   something you would want to inquire into in cross rather
25   than objecting at this time.

417

1   Do you withdraw your objection?
2   MS. MORGAN: Your honor, as long as it's clear
3   in the record that that came -- that he drew that fact
4   from Mr. Boback's testimony, then I will withdraw my
5   objection.
6   JUDGE CHAPPELL: I think that's clear based on
7   the form of the question.
8   Go ahead.
9   MR. MEHM: Yeah. Thank you, Your Honor.
10   BY MR. MEHM:
11   Q. Turning to factor four, Mr. Kam -- and that, as
12   you testified earlier to, deals with the mitigation of
13   risk -- to what extent could consumers have mitigated
14   the risk of identity theft or medical identity theft
15   created by the unauthorized disclosure of their personal
16   information in the 1718 File?
17   A. You know, as I mentioned earlier, consumers
18   have no way of knowing when an organization has a
19   disclosure unless they are notified by the organization
20   that had the breach.
21   In this case, my reading of Michael Daugherty's
22   testimony stated -- where he stated that they
23   decided -- LabMD decided not to go to notification;
24   therefore, these consumers, these 9300 consumers, whose
25   information was disclosed, whose sensitive personal

52 (Pages 414 to 417)

                                                                                    418

1   information was disclosed, had no opportunity to
2   understand that there was a risk and then to take the
3   appropriate actions to reduce the risk of falling victim
4   to identity crimes.
5   Q. So just to be clear for the record, is it your
6   testimony that consumers could not have mitigated the
7   risk of identity theft or medical identity theft created
8   by the unauthorized disclosure of their personal
9   information?
10   A. Yes.
11   Q. And I'd also just want to clarify for the record
12   that in looking at this factor, you also considered the
13   testimony of Mr. Daugherty.
14   A. Yes.
15   Q. So your analysis of the 1718 File is not based
16   solely of the P2P -- what you call the P2P disclosure is
17   not based solely on Mr. Boback's testimony; is that
18   correct?
19   A. That's correct.
20   And just for clarity, Ryan, I should add,
21   besides the two depositions that I had the opportunity
22   to review, I also looked at the research on identity
23   theft and medical identity theft, which is in my
24   literature review, which goes into extensive coverage of
25   what the potential injuries to consumers are from those

                                                                                    419

1   two instances, as part of my consideration.
2   JUDGE CHAPPELL: Who's Ryan?
3   MR. MEHM: Complaint counsel. That's me.
4   BY MR. MEHM:
5   Q. Why is it that a consumer could not have
6   mitigated the risk of identity theft or medical identity
7   theft in this instance?
8   A. They would have no way of knowing that their
9   sensitive personal information had been disclosed.
10   Q. And how does notice mitigate potential harm to
11   consumers?
12   A. Proper notice from an organization that has
13   breached information provides details to consumers on
14   the timing of the disclosure, as well as what
15   information was disclosed, like in this case name,
16   Social Security number, date of birth, and the like.
17   They also will typically prescribe certain
18   actions consumers can take based on the incident to
19   reduce their risk, whether it's contacting the credit
20   bureaus, whether it's setting fraud alerts, whether it's
21   contacting the organization itself.
22   A proper consumer notification will include many
23   if not all of these items to help a consumer understand
24   and assess their risk and take the appropriate actions
25   to reduce the risk.

                                                                                    420

1   Q. So even if LabMD had provided notice to
2   consumers regarding the unauthorized disclosure of their
3   information, their sensitive personal information in the
4   1718 File, would this have eliminated the risk of harm
5   to consumers from identity theft and medical identity
6   theft?
7   A. You know, unfortunately not.
8   What I've experienced is, consumers, even if
9   they do receive a notification letter from an
10   organization, they don't understand the risk that
11   they're facing, whether it's identity theft and more so
12   in the case of medical identity theft.
13   So unfortunately, even though they've been
14   alerted to the fact that there's been an issue, many
15   consumers don't take advantage of what an organization
16   might offer to help reduce the risk, putting them at an
17   elevated risk of falling victim to identity theft,
18   medical identity theft and identity crimes.
19   Q. And why is that?
20   A. You know, if I knew, I would love to tell you.
21   But from my personal experience working with
22   organizations who have lost hundreds of thousands or if
23   not billions of records of consumers, I think part of it
24   is consumers don't understand the risk, partly because
25   it's very complex. They don't understand what

                                                                                    421

1   organizations necessarily have their information.
2   But also part of the -- in the case of medical
3   identity theft, there's not many tools to identify those
4   risks, so, for example, there's no medical identity
5   bureau that monitors, you know, the -- a health
6   transaction and then alerts a consumer that there's been
7   potential misuse of their identity.
8   Q. Mr. Kam, what types of harms related to medical
9   identity theft are consumers likely to suffer from the
10   unauthorized disclosure of their information in the
11   1718 File?
12   A. It falls into three areas, financial harm, other
13   harms and reputational harm.
14   Q. Were you able to make a determination about the
15   risk of harm -- excuse -- strike that.
16   Were you able to make a determination about the
17   financial risk of harm from medical identity theft from
18   exposure of the 1718 File?
19   A. Yes.
20   Q. Were you able to estimate it?
21   A. Yes. I was able to estimate the estimated
22   out-of-pocket costs a consumer would experience.
23   Q. How many consumers, Mr. Kam, are likely to
24   become victims of medical identity theft as a result of
25   the exposure of the 1718 File?

422

1   A. I estimated 76 consumers out of the
2 9300 consumer records affected would fall victim to
3 medical identity theft.
4   **Q. Of these, of these, how many do you estimate**
5 **will experience financial, out-of-pocket losses?**
6   A. I estimated 27 individuals would have financial
7 repercussions, specifically out-of-pocket costs.
8   **Q. And on average, how much will each of those**
9 **27 victims suffer?**
10   A. On average, $18,660 of out-of-pocket costs.
11   **Q. And can you please break down for**
12 **Judge Chappell what that $18,660 in out-of-pocket costs**
13 **consist of.**
14   A. It consists of three things, the first being
15 victim -- the victim paying for service -- paying
16 providers for services that were given to the identity
17 thief or provided to the identity thief.
18   The second is for legal identity protection and
19 credit counseling.
20   And the third is to pay for medical services
21 because their health insurance has lapsed.
22   **Q. And what did you look at or consider to arrive**
23 **at this conclusion?**
24   A. You know, I looked at a range of research that
25 exists on medical identity theft, specifically starting

424

1 **applying the Ponemon study to your estimates?**
2   A. You know, when I looked at the calculation to
3 develop my estimates, I viewed the calculations to be
4 the floor, so the minimum, at least the minimum number
5 of people who might fall victim to identity theft, in
6 this case medical identity theft, as opposed to the
7 universe of all of the issues that an individual
8 consumer could see from medical identity theft.
9   **Q. And what was it in the Ponemon study that led**
10 **you to conclude that the financial out-of-pocket cost**
11 **estimates are a floor?**
12   A. Well, the Ponemon study specifically was -- its
13 objective was to identify the frequency and the impact
14 of medical identity theft on an average -- on a U.S.
15 citizen, on an average U.S. citizen, not necessarily
16 from someone who -- whose information was disclosed in
17 an unauthorized disclosure. And therefore, if you look
18 at the average risk an individual sees, it's the -- I
19 used it as the floor as opposed to the universe.
20   I think I mentioned earlier, people whose
21 information -- whose sensitive information is disclosed
22 because of a data breach has been shown through other
23 research to be at an elevated risk of identity theft and
24 medical identity theft.
25   Specifically, you know, there's been research

423

1 as -- with a report by Pam Dixon that was published in
2 2006.
3   I probably looked at a dozen or so research
4 reports, including from organizations like the
5 Bureau of Justice Statistics, Javelin Strategy and
6 Research, and others.
7   And what I concluded was the most -- the best
8 report to use that was applicable to this case was based
9 on research done by the Ponemon Institute, and so I
10 used --
11   **Q. And what --**
12   A. I'm sorry.
13   **Q. Excuse me. Please go ahead. Finish your**
14 **answer.**
15   A. I was going to say the 2013 Ponemon Institute
16 research study on medical identity theft.
17   **Q. And so that is what you concluded, just to be**
18 **clear for the record, would be the best study to apply**
19 **to the facts of this case?**
20   A. And -- it was. And specifically, it was the
21 only study that looked specifically at the harms the
22 victim would see from a financial and other harms
23 perspective. There was no other study I could find that
24 was as specific or as reliable as the Ponemon Institute.
25   **Q. Mr. Kam, what limitation exists with respect to**

425

1 done on identity theft, but not necessarily looking at
2 the information in terms of elevated risk for medical
3 identity theft from a breach.
4   So versus guessing and trying to pinpoint
5 whether a breach would increase the risk by some
6 percentage, what I decided to do so others could repeat
7 my analysis, if necessary, was to use the base rate or
8 factor for medical identity theft as identified in the
9 Ponemon Institute and use that to calculate the
10 76 consumers who are either today victims of identity --
11 medical identity theft or will become victims of medical
12 identity theft.
13   **Q. Given that the Ponemon study looked at financial**
14 **harm from medical identity theft across the entire U.S.**
15 **population instead of, as I understand it, focusing on a**
16 **smaller subset of breached consumers, why then did you**
17 **look to the Ponemon study?**
18   A. Because it literally is the only study I could
19 identify that provided the methodology or an estimate
20 that I could -- that was objective, quite honestly.
21   **Q. And just to be clear for the record, what does**
22 **that use of that methodology mean in terms of the**
23 **projections that you gave us a few minutes ago about the**
24 **76 and the 27 consumers?**
25   A. A way to think about it is that's the minimum

54 (Pages 422 to 425)

426

1   number or at least the number -- 76 is at least the
2   number of the victims who could be victims of medical
3   identity theft based on the formula that I used.
4   Q. And does that same formulation also -- the
5   "at least" formulation also apply to the 27 victims who
6   likely will suffer out-of-pocket -- financial
7   out-of-pocket costs for medical identity theft?
8   A. Yes.
9   Q. Mr. Kam, what role did ID Experts play in the
10   Ponemon study?
11   A. We were one of the sponsors of that particular
12   study.
13   Q. And as a sponsor, what say or influence did
14   ID Experts have over the study or its results or its
15   findings?
16   A. We have no -- we had no influence over that.
17   Q. You testified earlier, Mr. Kam, that consumers
18   are likely to suffer financial harms, I believe you
19   called it other harms, and reputational harms from the
20   exposure of the 1718 File.
21   What are some of the other harms that consumers
22   whose information was exposed in the 1718 File likely to
23   suffer?
24   A. The other harms are driven primarily by a
25   consumer's electronic or medical record being

427

1   compromised. And they include a misdiagnosis of
2   illness, delay in treatment, mistreatment, wrong
3   prescriptions prescribed, and the potential for
4   withdrawal of health insurance, loss of health
5   insurance.
6   Q. Mr. Kam, I'd like to turn now to a document that
7   has been marked as CXD 04.
8   And Mr. Owens, if you could please pull this
9   up.
10   And Mr. Kam, that document also should be in
11   your binder that's in front of you.
12   A. I see it, yes, I do.
13   Q. Mr. Kam, what is this document?
14   A. It describes the other harms from medical
15   identity theft consumers could see from an unauthorized
16   disclosure of their sensitive information.
17   Q. Is the information on CXD 04 contained within
18   your expert report?
19   A. Yes.
20   Q. Does CXD 04 accurately reflect the information
21   in your expert report?
22   A. Yes.
23   Q. And turning now to CXD 04, what does it show?
24   A. It shows the projected number of victims
25   suffering from other harms from medical identity theft,

428

1   and it goes through the various harms that I mentioned
2   earlier, identifying the specific number of victims that
3   I estimated for this case.
4   Q. So let's go down the chart and let's turn first
5   to the first row under the -- in the chart under the
6   headings -- under the heading Other Harms From Identity
7   Theft?
8   JUDGE CHAPPELL: How much more time do you think
9   you'll need for your direct?
10   MR. MEHM: Approximately one hour.
11   JUDGE CHAPPELL: All right. We're going to cut
12   off here in about five minutes, so proceed accordingly.
13   BY MR. MEHM:
14   Q. Turning to the first row of the demonstrative in
15   front of you, Mr. Kam, approximately how many consumers
16   whose information was exposed in the 1718 File are
17   projected to have an illness misdiagnosed as a result of
18   the incident?
19   A. I estimated 11.
20   Q. And what potential consequences could a consumer
21   experience from having an illness misdiagnosed?
22   A. It could be some very serious health
23   implications, including potential death of the
24   consumer.
25   Q. And approximately how many consumers whose

429

1   information was exposed in the 1718 File will experience
2   a delay in receiving medical treatment as a result of
3   the incident?
4   A. I estimated also 11.
5   Q. And what potential consequence or consequences
6   could a consumer experience from a delay in receiving
7   medical treatment?
8   A. You know, again, it could impact their ability
9   to receive timely healthcare, which could impact their
10   overall safety and again potentially result in death of
11   the consumer.
12   Q. And approximately how many consumers whose
13   information was exposed in the 1718 File will have an
14   illness mistreated as a result of the incident?
15   A. I estimated ten consumers.
16   Q. And what potential consequence or consequences
17   could a consumer experience from having an illness
18   misdiagnosed?
19   A. Well, in this case, yeah, I think you asked
20   about mistreatment?
21   Q. Yes. Excuse me. I'm sorry. Mistreatment.
22   A. So an example of that is, I mentioned if your
23   electronic health record or your medical record is
24   compromised. What happens is a victim's medical records
25   will merge with those of the identity thief, so if the

55 (Pages 426 to 429)

430

1   identity thief perhaps has a different blood type than
2   you do as the consumer, having the wrong blood
3   transfused in the emergency room can cause some serious
4   risks to health.
5   **Q. Mr. Kam, approximately how many consumers whose**
6   **information was exposed in the 1718 File will have the**
7   **wrong drug prescribed as a result of the incident?**
8   A. I estimated eight.
9   **Q. And what potential consequence could a consumer**
10   **experience from having the wrong drug prescribed?**
11   A. Serious threats to their health and safety, an
12   example of which could be a consumer who's allergic to
13   penicillin being prescribed penicillin and having a very
14   negative reaction to that.
15   **Q. And approximately how many consumers whose**
16   **information was exposed in the 1718 File will lose their**
17   **health insurance as a result of the incident?**
18   A. I estimated 30.
19   **Q. And what potential consequence could a consumer**
20   **experience from losing their health insurance?**
21   A. Risk to their health by not being able to get
22   access to timely medical services.
23   **Q. What did you base the projections in CXD 04 on?**
24   A. I based them on the information, the facts of
25   the LabMD case, the documents that I received from the

431

1   Federal Trade Commission, as well as the formulas that
2   were prescribed or defined in the research from the
3   Ponemon Institute, specifically the 2013 edition of the
4   Ponemon Institute's research on medical identity theft.
5   **Q. And specifically, are you referring to the**
6   **Ponemon 2013 Survey on Medical Identity Theft?**
7   A. Yes.
8   **Q. And what limitation, if any, exists regarding**
9   **the projections on the CXD 04?**
10   A. Much like I described for the financial
11   out-of-pocket, these estimates should be viewed as a
12   floor versus the total universe of all potential injury
13   these consumers can see.
14   MR. MEHM: Your Honor, this may be a good time
15   to conclude for today. I'm about to start on another
16   line of questioning.
17   JUDGE CHAPPELL: All right. We'll do that.
18   MR. MEHM: Thank you very much.
19   JUDGE CHAPPELL: We'll continue tomorrow at
20   0930.
21   We're in recess.
22   (Whereupon, the foregoing hearing was adjourned
23   at 5:33 p.m.)
24
25

432

1   C E R T I F I C A T I O N   O F   R E P O R T E R
2
3   DOCKET/FILE NUMBER: 9357
4   CASE TITLE: In Re LabMD, Inc.
5   HEARING DATE: May 21, 2014
6
7   I HEREBY CERTIFY that the transcript contained
8   herein is a full and accurate transcript of the notes
9   taken by me at the hearing on the above cause before the
10   FEDERAL TRADE COMMISSION to the best of my knowledge and
11   belief.
12
13   DATED: MAY 25, 2014
14
15
16   JOSETT F. WHALEN, RMR
17
18
19   C E R T I F I C A T I O N   O F   P R O O F R E A D E R
20
21   I HEREBY CERTIFY that I proofread the transcript
22   for accuracy in spelling, hyphenation, punctuation and
23   format.
24
25   ELIZABETH M. FARRELL

A

$1,000 413:11
$18,660 422:10,12
$50 413:10
$500 413:11
a.m 211:8
AARP 389:2
ability 220:10 225:7
  225:8 285:23
  286:3 323:13
  384:16 385:17
  398:6 400:14
  429:8
able 221:23 222:4
  227:20 243:25
  244:4,6 260:12,17
  264:7 268:19
  285:24 293:21
  312:20 313:23
  314:3 360:6 384:3
  421:14,16,20,21
  430:21
abnormal 222:22,24
  222:25
absence 333:15
absolute 357:21
absolutely 304:9
  305:1 390:3 397:6
abuse 385:12
academic 295:12
  303:18
accept 267:2
accepted 239:25
  266:24 325:21
  355:15
accepting 344:19
access 229:5 243:16
  243:19,20 245:17
  245:18 248:6
  253:4 254:20
  260:13,18 261:12
  262:5,7,10,13,16
  262:23,25 263:10
  263:15,21 264:5
  264:16 265:1,4,9
  265:17,18,20,23

266:3,4,7,7,9,13
266:15,19,23
267:4,7,10,13,17
267:19,24,25
268:2,8,12,20,21
268:24 269:2,7,15
269:16,21,24
270:3 271:16,17
271:23 272:4,10
273:2,2,7,14,16,21
273:22,25 274:1,2
285:8 287:12,15
292:13,17,19
293:6,6 295:18
298:14 312:3
313:24 314:4,18
314:20 318:24
336:21 355:25
356:4 384:10,17
384:17 395:16
402:5 409:3
430:22
accessed 406:11
accesses 283:23
accessible 228:11
accessing 250:5,12
  252:17 259:25
  260:9 284:3
accommodating
  357:18
account 287:3 340:2
  384:12 394:24,25
  394:25
accounts 382:22
  384:11 395:1,2
  414:3
accuracy 432:22
accurate 222:3
  230:17 261:11
  267:19 365:12,19
  371:10,13,24
  432:8
accurately 267:15
  273:11 427:20
achieve 291:3
achieved 292:15
acknowledge 336:21

acknowledged
  336:20
acknowledging
  359:13
acquired 415:22
Act 300:5
action 213:7 294:20
  300:1
actions 285:16,17,18
  286:18 299:23
  332:7 401:16
  418:3 419:18,24
activities 304:11
actual 263:2
add 328:17 403:16
  418:20
addition 263:14
  272:11 315:2
  334:5
additional 305:11
  314:23
Additionally 351:12
address 223:22
  227:3,5 228:24
  251:15 296:16,22
  296:23,25 297:17
  297:19 308:21
  340:1 346:23
  348:23 350:17
  410:3 412:17
  416:15
addressed 229:17
  229:20 246:1
  296:18 305:3
  307:18 318:9,20
addresses 293:1
  350:19 361:20
  411:17,18 416:2,7
adequate 250:4,11
  252:16 259:24
  260:8 293:4 295:8
  296:8 297:1
adequately 268:13
adhere 286:23
adjacent 340:8
adjourned 431:22
administration

333:11
administrative
  211:13 300:5
  318:24
admissibility 328:1
  330:2 369:13,14
  375:15
admissible 350:24
admission 350:22
  351:2
admitted 345:16
  369:17 371:7
  372:16 375:20
admitting 349:16
adopted 306:4
advance 292:18
advantage 420:15
adverse 353:18,22
  353:24
advise 351:23
  375:21
advisor 330:23
advisory 415:5
advocacy 382:18
advocates 382:18
Aetna 389:2
affect 285:18 286:19
  290:2 292:3
affidavit 367:2
affidavits 371:7
afternoon 311:9,10
  352:15,16 373:11
  377:8
agencies 379:4
agency 301:21,24
  332:5
aggregate 362:22
aggregated 335:21
aggregates 362:6
aging 218:18 408:2
ago 283:17 304:24
  306:12,14 323:10
  380:5 383:2 402:7
  411:6 425:23
agree 216:9 218:17
  218:20 221:25
  226:25 231:6

239:21 241:23
244:18 245:3
246:21 247:13
252:7 289:16,21
290:1 298:23
299:6
ahead 218:7 259:7
  259:21 302:4
  308:12,15 328:25
  331:10 351:17
  373:17 390:9
  394:5 417:8
  423:13
Air 332:21,23,24
ALAIN 212:5
alerted 420:14
alerts 419:20 421:6
aliases 361:20
align 233:20
Alison 277:2,4
  278:19
allegations 236:10
allegedly 323:4
allergic 430:12
alliance 387:7,11,12
  387:13 388:10
  390:21
allow 230:11 269:20
  292:17 330:3
  347:24 349:13
  367:21 371:7
allowed 252:22
  312:17 347:12
allowing 220:9
  286:2 347:24
  349:6,9,9
allows 286:4
aloud 315:16
amassing 243:14
ambiguity 344:22
AMERICA 211:1
American 390:20
  391:2,15
amount 273:20
  286:4 405:9
amounts 243:21,22
  307:6,9 411:15

analysis 214:23 407:1,8 409:21,24 418:15 425:7
analyst 332:2,9,11
analyzing 404:23
and/or 294:19
annotate 341:2
anonymous 227:7,8 227:9
ANSI 390:19
answer 261:16 262:6,8,12,18,24 263:1 264:18 265:2,6,11 266:21 267:22 268:22 271:20 276:4 280:1,7 281:24 296:6,10 300:23 301:2 304:7 323:17 368:24 410:5 423:14
answered 355:3,5 368:22
Anti-Fraud 389:4
antispyware 224:6
antivirus 221:20 247:25 248:2,8,12 297:7,8
anybody 216:13
apart 358:10,13,15
apologies 323:25 338:3
apologize 236:18 250:15 253:9 264:9 315:8 346:8 373:21 375:16 376:19 393:7
Appeals 329:23
appear 242:8 340:5 340:8 341:3,23 344:23 347:7,15 348:17 350:10 351:7 359:16 360:7 365:2 368:10 369:1 370:3 399:10
APPEARANCES

212:1 213:1
appeared 346:19 350:14 360:16 363:6 368:14
appearing 343:8
appears 340:2 347:10 350:12 361:22 363:7,21
Appendix 232:1 233:15 328:13
applicable 346:22 388:17 423:8
application 280:18 282:23 288:6,6 314:16,17,19,20
applications 223:5 281:1 314:10,11 314:14
applied 329:7 350:13
apply 295:16 327:8 423:18 426:5
applying 411:5 424:1
approach 275:19 320:14 338:5 405:4 407:7,19
appropriate 233:22 273:24 282:24 295:23 296:19 316:2,24 318:1,14 318:18 403:10 404:7,19 405:1 418:3 419:24
approximately 236:20 252:23 332:11 340:18 380:25 387:13 391:18 392:6 398:5 404:20 408:3 428:10,15 428:25 429:12 430:5,15
April 393:15 408:22
APT 221:10,13,16
area 228:14,17 230:18 379:22

areas 242:7,8 259:2 333:11 372:3 379:13 386:22 394:11,22 421:12
argue 327:10 337:7
argument 326:1
arrangements 292:18
arrested 416:7,15
arrive 407:10 422:22
arriving 230:13
articles 391:22,25 392:6,10 413:9
aside 350:5 386:10 404:16
asked 214:24 215:1 215:4,14,17 217:5 217:7,9 218:13 219:2,11,14 237:25 238:6,15 242:6 247:6 250:10 287:24 300:23 303:22 311:14 317:8 323:3,7,7,12 334:15 341:15,16 341:19,22,25 343:4 345:4 347:2 355:3 363:4,19,19 364:19 365:1,9,16 367:13,22 368:3,8 368:12,17,21,25 392:3 397:24 402:7,11 407:8,10 414:7 416:22 429:19
asking 323:16,17 345:3 349:1 357:2 363:17 366:14,16 409:13,14,18 415:4
aspect 296:9 385:9
aspects 231:11,12 327:7
asserted 370:23
assertions 409:16

assess 237:25 238:7 248:24 295:19 304:17 382:7 402:11 405:15,15 419:24
assessing 405:5 415:20
assessment 232:7,22 236:3 246:9 247:10,23,24 248:10,11,14,25 297:4,6,10,13 379:14 405:8 407:11,13 410:18 416:17
assessments 248:9 390:22
assign 383:15
assigned 220:15 363:15,18 365:1
assignment 355:16 365:8 366:4
assist 235:24 328:3 378:21
assistance 329:17 378:10 383:4
assisted 379:3
assisting 379:14,18 382:11
assists 252:7
associated 327:5 334:3 344:14 346:20 356:19 358:3 363:2,8,10 363:20,24 364:3,9 364:11,17,20 365:3
Association 387:1,4 389:3,4 391:10,11 391:15
assortment 356:20
assume 214:24 215:1,4,15,17 217:5,7,9 218:14 219:2,11
assumed 217:1,14 217:15 218:2,3,11

315:17
assuming 272:17 281:3
assumption 264:19 316:18,19 344:6 356:21
assumptions 216:1 219:14 315:22 344:16
Assurance 332:4
assure 329:20
attachment 287:4
attacker 318:24
attacks 293:8
attempt 353:20
attempting 345:16 349:12 370:21
attempts 223:22 248:5,15,18 249:5
attended 333:14
attention 239:18 270:13,23 278:17 288:11 311:11 315:7,9 340:22 381:24
attorney 300:22 330:23 382:17 383:17
Attorney's 334:4
attorneys 391:16
attribute 220:2,6
attributes 273:19,23
authenticate 227:10
authority 372:25
authorization 294:18,19 317:2
automated 361:5,8
automatically 361:11
available 235:18 246:17 247:7,18 256:13 313:1,3 345:21 356:5 402:4 414:17
Avenue 211:15 212:11,20 213:8
average 413:3 422:8

422:10 424:14,15
424:18
avoid 398:6 400:14
awake 255:23
aware 226:12,14
228:6 246:2
251:21,23 252:3
272:24 279:8,10
299:19 302:8
303:1,6 340:14
awareness 251:16
251:24 252:1,2
301:13

B

b 232:1 233:15
247:15 328:13
bachelor's 333:9
back 214:3,18
217:24 221:24
236:14 239:12
247:13 250:14
252:15 255:19
256:4 270:1 311:3
327:17 334:18
373:22,24 375:7
377:21 402:6
background 258:24
259:11 303:9
317:6 333:8
389:19
bad 365:24
balancing 308:18
Baltimore 332:16
333:10,14
bank 340:1 365:24
banks 388:14
Bar 391:15
barcode 305:10
base 340:10 425:7
430:23
based 221:2 222:3
225:5 228:16
230:18 234:3,3
242:4,4 265:7
266:24 267:2
271:14 305:15

314:9 317:16
319:6 322:14
324:10 326:14,18
326:20 335:14
336:23 340:12
348:14 349:5,7,25
359:7 362:25
366:8 371:25
377:15,16 380:2
389:24 409:15
410:1,19 416:17
417:6 418:15,17
419:18 423:8
426:3 430:24
baseless 327:20
basic 232:6 245:18
246:9 295:10,22
363:4
basically 244:21
245:10 273:4
326:17 360:2
379:13,19
basics 258:22
basis 225:9 292:15
317:4 318:16,17
326:12,13 327:6,8
329:25 382:9
393:21 416:11
basketball 286:6
batching 360:22,24
bay 398:5
bears 389:21
becoming 243:12
307:7 331:24
befall 379:15 405:12
began 233:24
236:15,25 331:21
beginning 243:8
382:5
begins 311:13
behalf 212:3,16
213:3 365:20
381:12 384:15
395:2
belief 432:11
believe 232:13
259:12 260:6

269:1 297:24
306:7 314:2 316:9
317:5,11,13 329:1
333:17 337:2
344:15 345:13
349:14 350:23
416:6 426:18
believed 403:4
416:23
belong 408:5
belonged 390:15
408:7
beneficial 292:20
294:5,23
benefit 338:16
345:12,18
benefits 412:6
best 240:9 309:8
387:17 388:15
423:7,18 432:10
better 376:24
beyond 251:24
257:11,20 259:11
315:22 316:7
367:16 389:7
413:12
big 232:23 234:10
bill 262:13 273:12
395:18
billboard 241:18
billing 261:12,15
262:4,10,16,21
263:14,20,23,24
264:16 265:1
266:20 267:5,24
268:9,25 272:18
273:10,13 314:16
411:15
billings 266:6
267:14,18 269:4
269:15 272:13,19
314:20,23 315:2
billion 414:10
billions 420:23
bills 372:4
binder 397:11,14
427:11

birth 346:22 361:19
394:18 396:4
405:21 411:12
419:16
bit 222:25 223:10
264:10 389:8
black 367:3 413:6,8
413:11
blood 430:1,2
Bloomberg 392:4,10
Blue 389:3,3
board 332:3,4,9,10
332:13,14 381:10
boards 390:14
Boback 408:24
409:7 415:25
416:20
benefits 412:6
Boback's 408:9,14
410:1 416:4,18
417:4 418:17
bodies 378:18
Boston 388:22
bottom 261:10
266:16 271:11
289:5,6 293:17
branch 332:20
breach 226:15 378:9
378:13,14,15,19
379:3,9 380:11,13
381:17 386:18
400:21,22 401:22
403:7 417:20
424:22 425:3,5
breached 403:2
419:13 425:16
breaches 380:25
406:19
breaching 378:22
break 255:2,4,7,14
258:13,17 260:2
305:18 310:8
327:17 373:8
375:3 422:11
briefly 389:16
400:12 406:3
bring 277:25 338:16
387:16

broad 367:21
brokerage 394:25
brought 258:1
browser 228:9,13
buildings 292:14
bullet 250:2
bureau 212:9
331:17 335:22
362:7 421:5 423:5
bureaus 362:19
364:7 419:20
business 223:13
235:15 243:13
262:22 263:22
284:2,3,6 290:23
303:24 333:11
334:6 382:16
386:20
businesses 223:14
245:22

C

c 214:1 250:3 252:15
259:24 274:7
377:25 378:1
432:1,1,19,19
calculate 425:9
calculation 424:2
calculations 424:3
call 257:15 258:21
259:9 292:17
309:25 354:21
372:17 375:9
376:17 379:24
380:1 418:16
called 214:10 221:6
221:10,13 225:11
241:18 247:10
256:23 292:8
321:24 331:7
377:4,12 388:12
408:2 426:19
calling 255:5 257:2
257:13 373:8
calls 288:18 291:20
330:15 367:12
camera 210:5,15

211:10 334:8
336:2,5,25 337:13
337:18,21 338:2
352:8 373:19
374:2 414:20,23
414:24 415:1,4,11
415:12
canceled 338:20
340:8
cancer 302:17
413:19
capture 245:23
312:19
captured 245:16
card 413:7,8
cards 395:3,3
care 231:9 234:24
255:7 257:8 303:2
309:20,20,24,25
310:3,5 349:16,17
383:8 387:3 389:4
391:11
careers 380:15
case 218:18 231:18
233:25 236:8,20
240:17 257:12
271:21 273:8,10
274:19 298:8
299:22 303:22
313:2 315:22
316:19 322:3,16
322:18,20 326:16
326:18 328:4,11
329:7,10,21 330:5
330:8 334:11,13
334:16 336:8,19
337:8,13 353:8
354:2,5,22 366:13
369:8 371:8
384:19 386:4,4
387:23 389:13,22
389:23 393:25
395:8 399:2,5
405:11,11,12
412:24 413:4
414:5 417:21
419:15 420:12

421:2 423:8,19
424:6 428:3
429:19 430:25
432:4
case-by-case 327:8
cases 340:1 382:8
384:7,20 385:13
categories 413:14
cause 213:7 225:12
225:14 320:2
404:9 412:3 430:3
432:9
caused 215:5
CBSNews.com
392:5
cells 367:3
center 218:18
379:24
central 406:25
407:2 409:19
certain 225:25
226:23 249:12
263:9 272:9
298:20 313:5
314:17,18 323:15
326:19 358:5
375:15 419:17
Certainly 339:8
344:10 351:16
certainty 357:21
certification 371:9
393:11,13,14
certifications 393:9
Certified 393:12
certify 367:3 432:7
432:21
CFR 325:22
chain 355:19
chair 397:11
chance 318:2 410:11
change 256:8
316:13 350:12
412:10,14,15,16
412:17,20 413:20
413:22 414:15
Chappell 211:12
214:3,6 215:8,11

215:18,25 216:4
216:15 217:12,19
217:22 218:6
219:9 228:4,6,16
228:20 229:1,4,9
229:11 238:10
241:17,21 255:3,9
255:13,19,21
256:15,18 257:1,4
257:17,25 258:14
258:18 259:20
261:19 270:6,9,14
270:20 275:21
276:2,6 277:21
278:4 283:15,22
284:7 285:6,11
286:5,13 287:1,11
287:16,22 300:21
302:4 305:15,19
305:25 306:7,11
306:16,25 307:12
307:21 308:12,14
309:2,7,18,23
310:2,7,13 311:3
316:4,11 317:4,9
317:16 319:5,17
319:23 320:4,12
320:15,17,22
321:3,6,10,14
322:12 324:10,14
325:2,6,11,13,17
326:2,9,12 327:13
327:16,24 328:16
328:25 329:11,13
330:13,22 331:1
331:10 333:4
336:6 337:16,18
338:7 339:5
342:14,17 343:24
344:8,11,17
345:13,23 346:5,9
346:12 347:11,22
348:25 349:5,15
349:22 350:3,19
351:9,14,17,19
352:1,5 353:12,21
354:7,12,17,20

355:4 357:13,19
366:20,23 367:19
368:23 369:3,9,12
369:24 370:24
371:2 372:19
373:2,4,9,14,16,22
375:2,7,11,22
376:4,12,15,20,24
379:11 384:5
387:21 388:1,7
389:8,24 390:4,9
392:13,16,20
393:1,4,21 394:1
396:22 397:2,22
398:18 399:17,23
399:25 409:10,13
409:25 410:7
412:5 415:3,7,9,15
416:11,21 417:6
419:2 422:12
428:8,11 431:17
431:19
characterize 284:5
285:14,19 381:8
411:19
chart 357:23 428:4
428:5
checking 384:11
394:24
checks 338:21 340:9
358:14 359:9
362:16
Chief 211:13
chilly 255:22
chip 305:7,10,12
chips 305:9
Christopher 253:12
253:14 254:6
261:2,5
CIPP 393:11
circles 239:2
circumstances
412:15
cite 235:1 246:16,16
246:20 274:23
275:5 276:13,23
277:9 306:24

307:11
cited 245:22 246:7
246:12 275:17
293:15 321:15
329:3
citizen 424:15,15
city 361:20
civil 275:25 335:24
362:23
clarification 324:13
344:12 347:18
clarify 253:20 260:7
277:16 278:5
311:18 315:21
403:18 415:3
418:11
clarity 216:5 418:20
Clay 256:11
clean 294:2
clear 258:20 261:20
270:15 287:2,25
307:21 309:18
321:19 322:4,12
323:25 329:22
334:24 335:1,2,7
335:11,17,21
336:22 342:11,14
342:19 343:4,4,9
344:18,25 345:2,4
345:6,7 346:16,19
347:3,8 349:3,22
349:24,25 351:6
353:12 359:3,3,4
359:12,24 360:22
360:23,24 361:10
361:10,16 362:5,6
362:9,12,18,22
363:4,23 364:2,5
364:11,16,16,19
364:19,23 365:5,9
365:20 366:8
367:2 370:13
371:10,24 372:1,2
373:24 376:8
399:17 404:2
409:2 417:2,6
418:5 423:18

425:21
CLEAR's 365:11,18
clearing 336:7
clearly 268:7 328:5
  372:23
clerk 330:20,22
clerks 261:12
click 228:8,12 287:4
  287:8
clicked 360:1
client 336:25 337:2
  344:4 379:9,12
  381:12
clients 302:21,23
  344:7,7 379:2
  403:2 406:18
close 283:3,5 381:4
  397:11
closed 336:9,15
closer 310:12
closing 245:15
co-conspirator
  285:12,15,20
codes 263:24 361:21
  411:14,14
coding 347:5 350:6
  350:13
coffee 264:11
cofounder 377:14
coined 237:17
colleague 338:4
collected 348:10
collects 396:16
  398:13,17
color 347:5 350:5,13
color-code 347:2
colors 347:12
  359:16
column 357:22
  358:8 392:3
combination 291:20
come 227:20 327:2
  327:11 370:15
comes 223:20 287:2
coming 233:24
  258:9,10,11,12,13
  265:12 282:11,17

282:21 283:12
298:7 332:1
comment 403:16
commission 210:1
  211:1,14 212:3,8
  331:20,25 332:1
  333:19 334:20
  335:3 338:25
  339:4 393:16
  402:24 411:3
  431:1 432:10
commit 394:19
  396:3 409:8
  411:22 412:1
  414:1
committing 416:8
common 235:8
commonly 247:8,18
commonplace 306:8
communicate
  290:22,23 291:14
  291:24 305:8
communicates
  291:16 292:1
communicating
  284:4
communication
  312:16,23
communications
  333:12 379:20
community 306:2,5
  306:9
companies 307:25
  399:3
company 221:6,9,13
  222:22 229:4
  273:12 286:5,7
  287:3 289:14
  290:3,4 291:7
  294:25 307:22
  313:23 314:3,5,12
  377:12,20,21,24
  378:2,6,12 380:5,9
  380:16 381:2
  394:7 396:15
  398:13,16 399:11
  408:10

company's 292:21
  292:22
company-related
  289:1,23
compare 357:25
compel 400:21
competition 337:11
competitively
  337:12
competitors 298:21
complaint 236:7,11
  236:16,17 237:1,2
  237:3,18 241:25
  242:4,4,9 247:5,14
  247:15,15 249:25
  250:3 321:15
  330:15 337:14
  339:11,20 341:12
  342:4 348:11
  350:22 355:10
  356:13 372:22
  373:12,12 376:16
  419:3
complete 263:22
complex 383:23
  407:13 420:25
compliance 332:2,9
  332:11 387:3
  391:11
complicit 286:1
comply 291:12
  301:14
complying 252:8
components 288:7
comprehensive
  233:21 237:10,14
  237:21 238:2,3,8
  238:19,22,24
  239:3,9,22,24
  240:4,10,15,24
  241:15 242:12,23
  243:1,24 244:1,7
  244:14 245:11
  250:17 290:17
  292:25 293:12,16
  295:3 300:18
  307:17 308:4

309:1 326:25
327:3,12
comprised 358:15
comprising 371:5
compromise 318:12
compromised
  384:23 427:1
  429:24
computer 221:17
  222:23 225:11,18
  225:18 226:1,1
  228:7,10,17,21,22
  229:6 234:20
  235:10 256:11
  280:2,5,18 282:25
  284:21 286:7
  405:3
computers 222:23
  222:25 223:14
  225:15 281:1,11
  282:23 284:3
  288:24 289:22
  293:7,23 294:6
computing 235:9,13
  245:6 292:4 305:7
  308:2 318:8
concentration
  333:11
concept 237:20,22
  238:3,4,8,18 239:5
concepts 245:14,16
concern 223:23
  257:17
concerned 257:7
  266:12 298:10
concerning 261:14
  262:10
concerns 369:21
  371:3,4
concise 321:19
conclude 219:17
  244:13 296:25
  336:3 410:25
  424:10 431:15
concluded 260:8
  265:25 423:7,17
concluding 320:23

conclusion 230:11
  233:24 234:4
  265:13 266:2
  272:8 282:21
  320:24 340:10
  404:11 422:23
conclusions 230:13
  230:19 233:11
  283:12 298:7
  326:15,17,20
conduct 352:2 353:4
conducted 304:10
  305:2 353:1
confer 319:18
conferences 391:7
confidential 298:14
Confidentiality
  298:11
configured 271:15
confirm 271:8
  341:22 343:7
confrontation 337:6
connect 398:23
connected 228:10
  228:13,14,23,25
connection 291:2
  317:14 416:15
consecutive 222:19
  224:5
consent 345:19
  351:23 368:7
  375:18
consequence 291:14
  291:16,17,24
  292:2 294:9 429:5
  429:16 430:9,19
consequences 230:1
  230:7 285:16
  290:14 291:17
  292:2 299:25,25
  385:5 428:20
  429:5,16
consider 231:1,16
  232:17 236:1,3
  263:8 272:2 288:1
  289:12,15 291:10
  292:20 309:12,25

326:19 328:11
329:19 404:12
415:23 422:22
consideration
231:22,25 328:18
372:24 419:1
considered 231:19
232:10,14,20,22
232:24 235:16
263:12,13,18
309:3 322:2,15
328:12 394:4
404:13,18 415:24
416:4,22 418:12
consist 422:13
consisted 335:10
consistent 235:4,6
235:13,14 244:21
244:25 295:11
296:4 306:23
326:15 343:14,17
consists 244:2,8
422:14
consult 302:3
consulting 303:23
consumer 212:9
266:9 315:22
316:18 331:17
334:5 378:23
380:1 388:22
389:6 394:9,10
396:7,14 398:12
398:15,22 399:2
400:17,24 402:4
405:24 406:9
412:9,11 419:5,22
419:23 421:6,22
422:2 424:8
428:20,24 429:6
429:11,17 430:2,9
430:12,19
consumer's 401:25
413:17 426:25
consumers 217:3
237:11 315:19
344:7 352:20,23
368:19 378:17,22

379:25 386:19
398:6 400:14,22
401:2,6,11,14,21
402:13 403:9
404:9,20 405:1,6
405:13,16 406:15
408:4 410:19
411:8 413:22,23
414:13,15 417:13
417:17,24,24
418:6,25 419:11
419:13,18 420:2,5
420:8,15,23,24
421:9,23 422:1
425:10,16,24
426:17,21 427:15
428:15,25 429:12
429:15 430:5,15
431:13
contact 368:19
369:1
contacting 419:19
419:21
contain 233:4 244:5
286:17 295:10
contained 240:25
263:16 274:8,22
275:3 294:6
335:16,21 339:21
341:7 347:25
359:8 361:15,17
361:18,22 368:15
400:7 411:8
413:14 427:17
432:7
contains 233:5
241:14 245:9
340:1,18
contemporary
278:20
content 286:12,17
286:22 287:8
contention 268:12
context 278:3,4
356:3
continue 239:12
304:22 316:10

321:4 325:2
337:19 371:4
373:25 414:1
431:19
continued 213:1
338:10
continuing 335:12
335:12
continuity 301:16
contradiction 273:1
contradicts 272:16
273:3,5
contrary 328:12
control 227:13
245:17 265:17,18
265:20 295:18
343:7 402:5
convictions 335:25
copied 360:1
copies 330:18,23
copy 215:23,24
320:12 338:5,6
339:14,17 345:21
corp 377:25 378:1
corporate 333:12
corporation 211:4
corporations 335:5
correct 214:24
217:10,11 218:11
218:19,22,25
221:14,18 223:15
223:18,21 225:1
225:15,23 226:3,9
226:21 227:23,24
229:14,23 230:2
230:22 231:18
232:11,17 233:17
234:1,5,14 235:19
235:23 236:6
237:12,15 238:16
238:20 242:13,17
248:12,22 249:6
249:25 251:22
252:9,18 254:6,13
254:23 256:17
262:8 264:21
265:2,6,11,19

266:21,23,25
268:9 271:9
272:10 273:14
275:22 276:5,14
276:16 278:21
283:10,20 284:16
287:11 288:3
289:19,24 290:5
293:4,13 298:8
300:17 301:9,14
301:18 303:21
316:22 323:1,5
324:5 344:25
345:1 352:18,19
352:20,22,24,25
353:2,3 354:15,16
355:11,20,21
356:4,8,9,11,24
358:12,14,18,19
358:23,25 359:5,6
359:9,20 360:5,10
361:8,9,13,15
362:1,3,15 363:12
365:7 371:23
372:12 415:14
418:18,19
corrected 342:19
correcting 276:3
correctly 247:11
261:17 263:6
271:25 282:7
289:2 291:22
309:2 343:8
360:21 361:25
362:11
correspond 341:23
corresponds 247:14
corrupted 384:25
cost 424:10
costs 421:22 422:7
422:10,12 426:7
cough 275:20
Council 235:2,11
246:10,24
counsel 247:6
277:18 302:3
319:17,25 321:15

330:15 334:13
336:17 337:14
339:11,20 341:12
345:20 346:4
348:11 350:22,25
355:10 356:13
357:10 366:2,10
366:11 368:17
372:22 373:12,13
376:16 419:3
counsel's 277:17
342:4 351:23
375:18
counseling 422:19
Counselor 320:5
337:17
counted 340:21
country 379:8
couple 246:7 250:14
257:23 267:22
383:2 394:11,22
400:13 401:20
course 223:13 297:7
298:13 366:12
380:15
court 211:19 257:9
257:20 312:13
314:2,15 315:25
318:5 329:9,23
330:20 331:15
335:9 337:4
339:24 347:5
349:2 351:4,23
362:20 377:9
389:19
court's 328:18
338:16 345:11
390:6 407:16
410:12
courtroom 255:21
325:25 330:17
336:7,13 345:20
courts 362:23
cover 298:4 299:22
coverage 276:25
297:6 418:24
covered 259:8

CPT 411:14
create 251:3 318:1
  348:15 363:14
  382:16
created 243:7
  305:22 358:25,25
  359:7,10 361:14
  361:15 369:20
  380:7 382:20
  417:15 418:7
creates 284:17
  301:13,16
creating 354:2
  359:17
creation 353:9
credentials 368:6
credibility 353:19
credit 335:22 362:7
  362:16,19 364:7
  395:2,3 413:7,8
  419:19 422:19
crimes 334:2 380:6
  394:19 401:24
  404:10 412:2
  414:2 418:4
  420:18
criminal 335:24
  362:24 372:5
  395:6
criminals 413:3
critical 409:23
crop 384:2
cross 210:8 241:19
  316:6,7,13 352:5
  353:13,18 354:18
  389:3 416:24
cross-exam 214:4
  305:16 352:2
cross-examination
  214:13 328:15
  352:13
current 251:14
  298:15
currently 251:13
  254:9 296:20
  377:11,17 386:23
Curt 274:14

customers 298:15
  358:6
cut 343:2 359:23
  428:11
CV 259:3,8,13
  303:14 392:13,17
CVs 259:1
CX 210:16 216:7,7,9
  261:5 270:24
  278:17 297:24
  298:5 311:13
  338:5,13,19,20
  339:10,14,19,21
  339:24 340:6,17
  340:18,21,22,24
  341:2,5,8,10,13,23
  341:24 342:8
  343:2,8 344:24
  345:12 346:19
  347:10 348:7,9,10
  348:15,17 350:7
  350:10,13,14,22
  351:3,8,24 353:11
  354:3 356:8,12
  357:1,4,12 358:16
  359:23 363:21
  365:3 366:17,19
  369:2,11,20 370:3
  371:3 372:16,25
  397:10,12,15
  414:22 415:1
CXD 427:7,17,20,23
  430:23 431:9

D

D 210:2 211:12
  212:18 214:1
  432:19
D.C 211:16 212:12
  212:22 213:10
daily 222:18 224:4
  224:12,18 225:8
  382:9 385:19
dashes 340:14
data 214:23 215:5
  219:3,5,13,15,19
  220:3,6 226:15

  227:14,15 230:10
  230:14,25 232:20
  234:5 235:3,12,18
  235:24 236:5
  240:25 241:25
  243:11,12,15,15
  243:16,19,21,22
  245:18 246:3,4,6
  246:11,15 279:14
  285:1,3 290:2,4
  291:1,7 292:5,21
  294:6,24 295:7
  296:8 297:1
  298:24 300:11
  301:22 303:24
  304:4 307:6,13
  312:16,19,23,23
  316:24 318:1
  319:2,14,15 322:7
  322:8 326:22
  327:9 328:7,21
  329:6 354:25
  371:5,10,24 372:1
  372:2 378:9,13,14
  378:15,19 380:13
  386:15,17 400:21
  403:6 405:20
  406:19 411:20,21
  413:2,14,21
  424:22
data-serving 227:15
database 263:4,16
  272:15 277:5
  314:24 342:11,11
  342:14,17,19,20
  342:20,24 343:18
  344:25 345:2,4
  346:18 349:4
  350:9 351:7
  361:10 370:13
date 341:9,10
  346:21,22 364:14
  394:17 396:4
  405:21 419:16
  432:5
DATED 432:13
dates 224:17,23

  341:7 361:19,19
  411:12
Daugherty 358:6
  418:13
Daugherty's 337:15
  417:21
day 220:24,24 221:1
  223:25 251:12
  257:8,8 338:22
  346:2 355:9,13,17
  355:20,25 356:4,5
  356:10,12,16,18
  356:19,23 358:1
  358:10,13 359:8
  359:19 360:5
  363:6 367:7 368:1
  368:5,10,14,20
  370:4,11 371:22
day-to-day 378:4
days 222:19 224:5
  383:2
deal 375:10 406:19
dealing 327:9
  333:25
deals 417:12
dealt 328:22
Dean 256:13
death 346:22 361:20
  428:23 429:10
decade 385:18
decided 388:16,22
  417:23,23 425:6
deciding 329:10
decision 322:2,15
  329:21
defense 305:21,22
  306:1 307:14,16
  307:21,24 308:7
  308:11,24,25
  309:3,5,12,17,19
  309:23 310:3,5
  317:14 320:2
  327:4
define 239:9 283:24
  283:25 295:13
defined 229:22
  431:2

defining 290:16
  311:25 312:2
definition 239:21,23
  239:25 240:2,14
  240:19,20,23
  241:14 244:15
  287:2 293:11,15
  327:3
definitive 220:16,21
  220:23 221:1
definitively 363:14
  363:18
defraud 414:8
defrauded 414:10
degree 333:9
degrees 255:24
delay 330:18 351:4
  376:19 427:2
  429:2,6
delaying 384:16
deleted 282:5
deliberately 367:4
delineating 241:25
demand 275:25
demonstrate 385:16
  396:24 397:4,24
demonstrative
  428:14
denoted 367:3
department 256:12
  262:5,10,16,21
  263:21 264:16,17
  265:9 266:18,20
  266:22 267:4,5,7
  267:17,18,24,25
  268:8,9,24,25
  269:4,5,7 272:13
  272:19,21 339:13
  355:14,18,23
  358:12,17,22
  370:5
departments 268:14
deploy 306:5 308:1
  308:9,24 309:15
deposition 236:24
  238:12 253:5,12
  254:10 260:23

275:15,24 278:19 279:22 303:10 360:14
depositions 418:21
depth 233:8 305:21 305:22 306:1 307:14,17,22 308:7,11,24,25 309:3,6,12,17,19 309:23 310:3,6 317:14 320:3 327:5
derived 406:16
describe 331:23 333:8,20 335:9 342:7,23 343:11 345:6 346:16 347:5 349:2 378:2 382:25 383:20 387:25 394:20 395:20,23 404:22 406:3 407:14 413:22
described 227:21 229:25 327:3 333:17 339:22 369:19 411:1 431:10
describes 327:11 427:14
describing 339:23 382:6
designated 356:6
desks 293:23
desktop 288:1
despite 265:22
detail 215:14
detailed 216:1
details 338:23 368:16 419:13
detect 248:1 396:9 396:11,13
detection 302:17
determination 222:8 228:3 252:21 253:4 285:3 323:19,23

324:2 330:6 421:14,16
determine 219:21 221:23 222:4 230:14 249:9 250:10 251:14 252:23 253:2 263:23 314:9,20 315:1 323:14 326:14 329:24 341:16 342:1,7,12 342:25 343:5,12 356:13 358:2 364:9 365:1 368:3 368:8,12,17 379:14 407:4
determined 364:2
determining 247:17 296:13
develop 237:9 245:11 388:14 424:3
developed 382:16
developing 240:10 242:12
development 379:19
devise 308:17
diagnosed 413:18
diagnostic 411:14
different 223:4 225:14,22,22 235:14 260:16 296:5 297:7,11,13 302:15 341:18 342:2,9 345:9 348:18 356:15 361:4 363:10 365:4 367:4 370:7 372:11 430:1
difficult 396:7,11,13 398:25
difficulty 400:17
digits 372:6
Dinsmore 212:19
direct 210:8 239:18 278:17 288:11 315:6,9 316:6,12

328:15 331:12 338:10 340:22 351:20 353:14 377:6 398:8 428:9
directed 355:15
directing 311:11
direction 334:13 356:13
directly 299:18,21 357:23 389:21 396:21
disability 371:11,12
disabled 274:8,22 275:4,10
discern 323:4
disciplinary 294:20 332:7
disclaimer 371:12
disclose 337:4
disclosed 317:2 380:3 394:10 396:8 400:18,24 401:22 402:1,13 405:19 406:1,9 407:6 411:7 417:25 418:1 419:9,15 424:16 424:21
disclosing 217:4 315:20
disclosure 317:13 318:2 378:16 379:10 380:10 394:8 396:8 401:4 401:8 402:14 404:21,24,24 406:6,7 407:1,24 410:23 413:24 415:21 417:15,19 418:8,16 419:14 420:2 421:10 424:17 427:16
disclosures 381:1 403:14
discovered 283:4,5 409:1,2
discuss 240:11

409:21 414:21
discussed 237:19 238:10 300:15
discussing 235:18 259:23
discussion 216:17 258:15 290:8 299:13 326:6
discussions 407:2
display 345:12
dispositive 330:4
dispute 353:21 376:11
disregard 389:25
disregarded 322:2 322:14
dissertations 259:2
distinguish 350:14
distributed 399:7
division 212:10 331:18 333:18,21 333:23 334:1
divulge 298:18
Dixon 423:1
Docket 211:4 214:3
DOCKET/FILE 432:3
doctor's 399:9
doctors 302:14 304:2,14
document 232:7,18 232:21,23 235:1 237:4 241:3,4,9,10 241:13 242:22 245:9,25 246:24 246:25 292:7 295:10 338:6,12 338:14,25 339:18 341:9,25 345:15 345:18 346:1,2,3 347:14,15,20 348:1,6,9,12 349:9 349:10,13,18,23 349:24 350:6,12 351:2,6,13,15 352:7 353:10 354:2,14 358:1,15

359:7,14,15,17 363:7,13,17 366:18 367:8 369:1,7,21,23,25 370:2 371:2,17 372:9,14 397:16 397:21 414:25 427:6,10,13
documentation 251:24 252:1,2
documented 314:8
documents 232:6 233:18,19 234:9 234:10,11 236:15 236:19,21 237:1 239:13 242:19 243:2,6,6,8 244:4 244:13,16 246:7 246:12,14,16,19 246:21,22,23,24 307:10 323:4 327:1 330:18 336:4 339:3,12 341:7 355:23 357:15 358:11,16 370:5 372:4 402:23 411:3 415:10 430:25
doing 214:23 223:3 244:12 245:11,14 245:23 251:13 258:24 286:23 296:20,20 297:5 297:12,14 299:19 299:25 360:25 363:1
dollar 413:8
dollars 414:10
domain 244:20
domains 235:9,15
door 283:20
dots 398:23
download 220:10 284:3 285:21,23
downloaded 283:23 284:16,21 285:11
downloading 220:19

284:10,13 286:1,2
286:11,15,17
287:25 299:17
downloads 283:19
dozen 423:3
dozens 399:13
Dr 229:21 230:12
320:19 325:6,11
325:13,21 326:10
326:13,17
draft 329:20
drafted 397:21
dragged 360:1
draw 266:2 270:13
270:23 362:16
drawn 306:18
draws 362:12,12,20
364:23 370:13
drew 417:3
drive 339:20 356:6
driven 426:24
drops 275:20
drug 430:7,10
drugs 395:17
due 219:12,18
220:18
duly 214:11 331:8
377:5
duration 318:21
duties 298:20
356:11
Dyke 256:7 258:9

E

E 210:2 214:1,1
311:1,1 432:1,1,1
432:19,19,19
e-mail 287:2,3,6,16
287:17,18 288:18
288:22 289:19
291:6 353:4
401:16
e-mails 291:20
E4 333:4,4
E5 333:5
earlier 306:25
315:11 329:14

355:8 364:5 371:3
371:6 382:10
391:13 393:2,5,6
411:2 414:2,6,7
415:21 417:12,17
424:20 426:17
428:2
earliest 341:9
early 246:13 289:17
ease 351:25
easier 249:20
327:17 335:13
336:16
easily 372:5
ecosystem 399:8
edition 431:3
educate 386:19
389:6
education 317:6
326:14 335:12
educational 258:24
259:11 333:8
effect 282:4 416:19
effective 271:24
306:5 308:10
309:6
effectively 222:21
229:9 296:21
eight 413:3 430:8
either 223:18
236:22 254:3
269:6 277:9 366:6
381:10 425:10
electronic 292:13
293:8 305:10
339:19 384:21
399:6 426:25
429:23
electronically 303:3
345:22
elements 240:18
405:20 416:3,22
elevated 401:23
420:17 424:23
425:2
elicit 347:19 399:19
elicited 344:15

400:2
eliciting 389:16
eliminate 282:24
401:10
eliminated 420:4
ELIZABETH
432:25
else's 412:6
embarrassed 385:12
embarrassment
412:3
embedded 245:2
286:12,22 288:8
emergency 235:10
430:3
emerging 243:11,20
243:21 251:12
295:20 307:6
emits 305:8
empathetic 383:6
385:16
empathy 386:6
employ 377:18
employed 251:9
265:8 377:11
employee 220:15
253:15 260:13,13
260:15 261:25
262:1 268:17,17
273:15 278:9,13
283:13,23 285:11
286:3 287:3,21
288:10,24 290:13
290:21 299:24
313:5 353:22
406:7,8
employees 220:9
250:4,12 251:19
252:17 253:3
254:20 259:25
260:9,16,18 262:9
262:21 263:10,21
264:5,16 266:3
269:25 270:3
271:16,17 272:4,9
272:13,17,18
273:8,10,13 275:1

290:22 291:3
294:14,16 301:14
313:24 314:4,23
employer 313:9
employment 303:9
331:23
encompass 244:10
encompasses 411:6
encounter 308:21
encouraged 303:2
enforce 240:7,9
250:23 252:6
290:19 308:6
enforced 265:16
enforcement 250:23
287:20 299:10,12
301:17,21,24
307:19 342:11,17
342:19 372:4
416:8
engage 380:9 382:8
engages 382:4
engaging 388:22
English 217:22
enlarge 254:16
288:12,14,15
292:9
entered 285:2 343:9
343:25 344:23
entering 343:21
344:13
entire 300:18
425:14
entities 246:1
entitled 398:5
entity 227:10,12
231:24 312:24
328:22 380:9
entries 358:8
environment 255:22
304:17
equal 321:23
equipment 293:23
293:24 294:17
equipped 292:13
equivalents 377:19
eradicate 221:17

223:18,20
eradicated 223:17
223:24 224:2,9,11
225:1,4
error 313:14
escape 220:2,6
escaped 219:3,12,17
219:22,25 220:2
220:18 323:5,15
especially 414:18
ESQ 212:4,5,6,7,17
212:18 213:4,5,6
essentially 380:18
383:3,12 384:16
385:1 387:17
389:5 394:23
405:5 413:17
establish 319:19
320:1 328:6
established 232:15
298:5 329:7
393:23,25
establishing 250:17
estate 362:21 372:3
estimate 421:20,21
422:4 425:19
estimated 421:21
422:1,6 428:3,19
429:4,15 430:8,18
estimates 424:1,3,11
431:11
evaluated 315:1
evaluating 315:4
event 258:2 329:22
380:22
events 381:3
EVID 210:15
evidence 219:17
220:17,21,23
221:1 224:11
225:3 226:17
227:17,18,19
230:6,9 233:25
248:3,4 252:22
253:1 265:15
285:1 325:23
328:13 330:3

348:1 355:19
371:8 397:23
evolve 251:14
exact 223:25 224:5,6
224:17,23 237:23
243:17 244:7,9
245:14
exactly 219:24
222:14 253:2
259:15 269:8
275:12,13 276:16
279:5 281:14
282:15 321:5,9
370:1
examination 214:10
257:22 311:7
324:16 330:19
331:7,12 336:3
338:10 351:25
357:9 377:4,6
414:21
examined 214:11
331:8 377:5
examining 300:22
example 228:8
286:6,15 299:17
312:18 314:16
371:6 385:12
389:17 421:4
429:22 430:12
examples 297:16
384:6
exceed 296:1
excerpt 261:5
excluding 307:4
exclusion 235:17,17
369:7
excuse 232:3 241:8
270:8 280:10
293:19 301:24
325:12 348:9
370:6 387:21
395:21 405:15
407:16 409:10
410:12 421:15
423:13 429:21
excused 325:7 337:5

372:20
executed 287:9
executive 378:3,5,7
380:16 381:10,13
381:18 382:1,2
exercise 309:19
exercising 309:24
exhibit 216:7 253:20
253:23 254:3
259:14 261:5
264:13 353:15
369:10
exhibits 210:15
215:12 375:15
exist 326:18
existing 296:15,17
384:11 394:24
exists 422:25 423:25
431:8
exit 336:12
exited 325:25
expect 223:7 255:4,7
258:20 259:9,9,16
313:9,11,21
expectations 301:22
expected 295:15,16
295:18,19 301:14
expecting 259:3
expects 284:6
Experian 362:16
experience 306:22
317:6 326:15
328:20 329:2,5
335:14 380:13
385:6,19 386:10
389:20 395:24
396:1 402:25
406:17 410:14
420:21 421:22
422:5 428:21
429:1,6,17 430:10
430:20
experienced 222:5
222:10 381:16
420:8
experiences 386:7
394:8

expert 237:3 256:21
256:24 257:9
258:21 295:9
309:8 311:12
313:8 315:7,9
317:10 321:19
322:19,20 325:21
326:10 327:22
328:2 329:16,16
329:16,17,18,18
329:22 366:12,13
367:12 370:8
383:8 393:5,18
394:2 396:18
397:20 399:20
400:3 427:18,21
expert's 328:2
392:11
expertise 367:17,17
392:12 393:22,24
experts 258:19
377:12,14,15,17
377:22 378:8
379:3,9,11 380:10
380:18 381:1
382:10 383:20
386:11 426:9,14
explain 220:8 268:5
306:5 312:13
314:2,15 318:5
379:10 388:6
explained 315:25
explanation 291:3
explicit 297:15,16
exploited 249:17
308:23
explore 350:2
exposed 217:8 226:1
227:11 412:12
426:22 428:16
429:1,13 430:6,16
exposure 318:11,23
319:14 322:7
407:23 410:19
414:14 421:18,25
426:20
expound 339:23

expressed 239:1
398:15
expunge 382:21
extended 412:22
extensive 328:12
418:24
extent 256:22
369:20 371:17
394:3 405:19
411:7 412:9
417:13
external 227:10,12
312:24
extract 314:24
extracted 315:1
extremely 385:8
eyes 356:6

F

F 211:19 311:1
432:1,1,16,19,19
432:19
face 372:8 382:7
facilities 292:12
304:2,6
facing 381:21
420:11
fact 267:2 272:11
275:25 286:21
290:2,3 291:10
293:3 298:6 303:2
318:9,23 326:16
326:18,19,24
328:4,8,18 337:9
353:23 371:10,10
383:13 401:19,25
417:3 420:14
factor 406:2 411:5
417:11 418:12
425:8
factors 405:14,17
406:4,5,16 407:14
411:1,4 415:19,20
416:5,18
facts 326:16,18
328:11 389:22
405:10 409:14,22

423:19 430:24
factual 366:14
409:16
failed 316:1
failure 291:12
316:24 400:20
403:9 404:6,18,25
fair 218:9 220:1
230:15 233:9,13
233:23 242:3,6
253:14 261:11
264:15,18 353:5
354:24 355:10,14
356:17,23 360:3
360:17,19,23
361:6,11 362:14
362:17 363:3,11
363:23 364:1,22
365:22 366:5
368:18
fairly 413:15
fall 252:8 380:6
385:10 386:8
422:2 424:5
fallen 380:23 383:14
385:24
falling 400:25
401:23 418:3
420:17
falls 369:15 379:13
382:14 394:11,22
421:12
familiar 220:24
231:13 236:10
306:14 334:23
family 368:5
far 257:7 293:5
298:10 347:25
349:16 353:19
Fargo 365:25
FARRELL 432:25
fates 375:2
Fe 390:21
February 332:25
408:10,13,18
federal 210:1 211:1
211:14 212:3,8

303:1 325:23
331:16,20,25
332:1 333:19,22
334:20 335:3
338:25 339:4
379:4 402:24
411:3 416:8 431:1
432:10
feel 255:24 258:22
264:5 307:15
319:1 385:11,13
386:1 400:4,4
feels 337:4
felt 376:24
field 247:10 328:7
328:20 393:18
fight 387:18 388:15
388:23
fighting 388:19
figure 268:11
figured 249:19
file 218:14,17,18,21
218:22,25 219:2
219:11,17,22
220:18,21 286:11
312:11,17,21
358:24,25 384:17
384:21 407:23,25
408:1,2,5,8,12,16
408:18 409:1,6
410:20 411:9,10
412:12,14 413:15
414:22 416:2
417:16 418:15
420:4 421:11,18
421:25 426:20,22
428:16 429:1,13
430:6,16
file-sharing 280:18
282:22,23
filed 375:23,24
376:2
filing 375:17 376:1
finally 249:19
finance 271:16
financial 271:17
272:17 334:2

379:6 388:13,15
388:18,19 394:18
394:23 395:12
396:1 412:2 414:4
421:12,17 422:5,6
423:22 424:10
425:13 426:6,18
431:10
financing 362:21
find 233:18 239:5
240:14,18 244:1,4
244:6,9,9 245:2,4
282:20 295:7
307:1,3,4 319:25
321:18,20,22
322:17 329:17,18
329:25 360:25
361:3 371:14
408:12 423:23
finding 250:10
322:14 376:19
findings 347:15
426:15
fine 276:6 357:11,13
357:16 366:24
finish 257:18 423:13
finished 325:4
336:15 362:2
finishes 258:4
finishing 258:6
firewall 248:3,7,7
248:20 249:4
275:2 277:11
282:1
firewalls 248:15
274:7,21 275:4,10
276:24 277:7
278:25 279:4,9
firm 332:15
first 237:1 246:21
246:23 257:8
286:7,9 306:7
321:17,20 331:7
338:20 339:22,25
346:2,24 377:4
379:13 381:9
382:4 398:9 404:3

406:2 408:10
411:5,11 422:14
428:4,5,14
first-class 401:15
fits 308:25
fitting 293:20
five 306:12,14
339:22,25 428:12
fix 216:16 225:11
flavor 389:19
flaws 296:14
floor 424:4,11,19
431:12
flowed 227:25
fly 346:6,7
focus 387:10
focused 235:12
focusing 425:15
folder 298:1
follow 309:10
375:22
follow-up 214:19
215:25
followed 290:3
291:5,8 294:13,23
298:24 299:1
300:11 313:10,12
313:20
following 223:25
271:13 311:16
338:1 375:25
follows 214:12
218:1 292:24
309:11,14 331:8
377:5
footnote 274:12,12
Forbes 392:5
Force 332:21,23,24
forces 389:5
foregoing 431:22
foreseeable 247:8
247:19
forgot 250:14
form 237:20 243:3
341:5 360:17
400:6 417:7
formally 394:2

format 339:19
340:14 348:11
409:1 432:23
formation 388:8
formed 388:2
forms 335:23
383:10 412:1
formula 426:3
formulas 431:1
formulate 236:16
306:19
formulated 263:9
327:1
formulating 226:20
232:10 236:8
260:24 272:3
274:18 275:15
formulation 231:17
235:25,25 306:17
426:4,5
forth 239:12 395:3
forty 387:13
forward 344:8
found 222:24 223:1
234:9 268:1
280:18 281:10,13
282:21 283:1
306:23 320:19
321:1,5 364:21
376:22 377:20
408:8,10,15,16,19
408:20,21,22,23
409:5,6 416:1,2
foundation 317:17
317:21 343:20
345:17 349:12
351:15 352:6
353:14 354:14
371:14 396:24
397:23
founded 377:21
381:2 389:13
founding 389:7
four 338:20 340:13
405:14,17 406:16
407:14 411:1
416:2,7 417:11

four-factor 405:7
fourth 406:13
frame 323:13
fraud 387:7,11,12
387:19 388:10,15
388:19,24 414:12
419:20
fraudulently 395:18
412:6
free 258:22
frequency 405:10
424:13
frequently 396:2
Friday 256:5,7,13
257:15,18 258:2,7
258:11,12
friends 368:5
front 239:14 427:11
428:15
frosty 255:23
FTC 230:24 231:1
235:19 236:5
241:1,5,10 301:25
339:20,20 340:12
352:17 353:21
354:4,10 355:13
355:16 356:6
358:11,17 370:17
402:9,11 407:8
FTC's 241:2 354:25
FTP 227:7,8,9
full 276:21 352:17
360:17 405:21
411:11,12 432:8
full-time 377:19
fully 293:20 385:4
function 284:2
360:22
functional 248:2
functionality 279:9
279:11
functions 263:23
333:23 352:18
378:6
further 214:12
260:7 305:14
319:3 324:9 325:1

389:10
future 415:9

G

g 213:4 214:1
  311:19
gain 248:5 395:13
  412:2 414:4
game 286:8,10
  399:18
gather 261:14
gathered 365:5
gender 346:22
  361:20
general 244:20,24
  245:4,5,16 264:20
  297:2,3,12 346:3
  347:15
generally 307:1
  411:19,21 412:10
  412:13
generated 272:20
generates 362:5,10
Georgetown 256:12
getting 235:22
  388:14 390:9
gift 395:3
gist 390:1
give 244:5 297:16
  299:18 317:7
  320:12 329:18
given 227:9 238:1
  242:8 249:15
  263:1 272:14,19
  273:2,2,6 282:12
  297:20 308:23
  318:7 355:13
  356:22 385:22
  386:5 422:16
  425:13
gives 246:5
giving 286:3 311:25
  415:4
glean 244:15
go 214:18 218:7
  224:20 239:11
  247:13 250:14

252:15 253:8
254:25 255:10
257:11,19 258:22
259:7,10,21 260:7
266:19 277:15
278:15 280:14
298:2,10 302:4
303:3 308:12,15
316:7 325:3,18
328:25 331:10
334:8 336:2,9
351:17 357:1,11
373:17 385:23
390:9 394:5 400:5
405:9 406:3
414:20 417:8,23
423:13 428:4
goal 290:8,10,10,13
  295:6 387:15,16
goals 240:5,6 290:18
  291:2 308:3,7,19
goes 258:21 270:1
  330:1 418:24
  428:1
going 243:25 252:5
  254:2 255:3,16
  256:5,7,8,14 257:1
  257:17,19,20
  259:1 285:18
  288:11 299:3
  325:2,18 327:17
  329:15 330:3,5
  331:2 336:7,9,12
  336:16 344:8,11
  344:18 346:5,7
  347:12 351:24
  357:6 366:20
  373:9 375:3 386:6
  389:25 409:16,20
  423:15 428:11
gold 309:3,6
good 214:15,16
  248:21 311:9,10
  352:15,16 372:13
  373:7,11 377:8
  431:14
goods 395:17

Gotcha 390:11
government 230:21
  232:10,13 233:14
  234:19 246:2
  301:25 303:2
  392:3
governmental
  295:12
governs 231:7,7,11
  231:12
graduate 333:13
grant 304:20,21
grant-related
  304:23
granted 336:5
  414:23 415:1
greater 318:13
grounds 389:12
  393:22
group 334:2,3 388:2
  389:9 390:21
groups 267:9 386:15
  386:22 389:17
  390:18,24
guess 296:5 371:9
  390:5
guessing 425:4
guidance 234:11
  251:8 376:1
guide 380:20
guidelines 230:20
  230:22,24 231:2
  231:17 233:11,19
  234:8,14 235:3,4,8
  235:9,13,24 236:1
  242:20 244:10,19
  244:21,25 245:17
  245:21,22 246:5
  250:24 295:22,25
  296:1,4 301:9
  306:19,23 307:2
  329:4
guides 406:22
guy 216:15

H

half 310:11 398:5

HALLEE 213:5
handbook 288:10
  289:13 290:21
handbooks 283:13
  289:9
handed 338:12
handful 380:14
  390:7,8
handwritten 340:24
Hang 373:18
happen 216:15
  284:14 286:4
  380:12 383:3
  385:13 388:24
  407:4,4
happened 249:8,10
  249:11,12,15
happening 279:25
happens 223:11
  381:15 386:1
  429:24
happy 351:21
hard 339:14
harm 214:24 215:2
  215:4,17 217:2,6,7
  217:10 218:10
  315:18,22 316:18
  317:8 320:2
  398:24 401:11
  402:2,16,19 403:9
  403:13,13 404:23
  405:5,15 406:14
  406:25 409:21
  410:19,22 412:4
  413:23 414:14
  419:10 420:4
  421:12,13,15,17
  425:14
harms 379:15 394:9
  394:20,23 395:9
  395:20,23 396:1
  398:6 400:14
  405:12 421:8,13
  423:21,22 426:18
  426:19,19,21,24
  427:14,25 428:1,6
HCCA 387:4

heading 288:21
  292:8 398:4
  399:16 428:6
headings 428:6
heads-up 415:6
health 300:4,12
  302:20 328:22
  384:21 387:3,5
  389:3 391:11,12
  392:3 396:5,5,6
  399:6,11 405:22
  405:23,24 411:16
  411:17,17 413:4,5
  413:10,17,18
  414:5,18 421:5
  422:21 427:4,4
  428:22 429:23
  430:4,11,17,20,21
health-related 231:8
healthcare 246:1,3,4
  246:6 300:6,7,9
  344:4 379:6
  388:20,25 399:8,9
  429:9
hear 259:12 306:25
  320:4 326:1 337:1
  351:5 356:2
  392:15,20 399:23
  399:24
heard 256:6 305:21
  316:7,11 323:20
  337:11 371:25
hearing 274:13
  275:25 276:14
  399:22 431:22
  432:5,9
hearsay 370:12,12
  370:12,12
held 337:20 338:1
  393:14
help 236:13 261:15
  319:17 335:13
  380:18 381:24
  383:12,18 385:2
  385:17 386:19
  387:17 388:6
  419:23 420:16

helped 363:14 379:4
384:8 385:20
helpful 294:15
328:8 329:9
330:21
helping 378:24
380:6,22 381:19
382:6,19
hepatitis 413:19
herpes 413:19
heterogeneous
308:8
high 229:22 249:18
413:6
high-level 318:19
high-risk 226:23
227:3 229:13
highest 308:19
Hill 210:9 214:9,15
215:21 216:6,9,19
217:5 218:13
221:5 229:21
230:12 232:2,9
236:7 239:15,18
240:14 241:23
253:11 259:23
276:8 283:8 284:9
289:12 292:10
294:4,22 295:2
298:3,4,23 299:7
300:10,15 301:3
301:20 303:8
305:13 311:9,22
312:9 313:4,22
315:6,25 316:17
317:13,24 319:12
320:19 322:5,25
324:18 325:5,6,11
326:10,13,17
328:10,12,19
329:2 379:5
Hill's 277:19 301:1
317:6 325:13,21
327:21 328:5
HIMSS 387:6
391:12
HIPAA 231:3,4,6,11

231:13,16,19,20
232:6,7 235:17
236:2 246:8,22,23
246:25 300:5
HIPAA's 231:16
HIPAA-covered
231:24
hired 271:5
history 251:7
331:23 396:6
412:20
HIV 413:19
HL7 279:12,13,15
279:18,19
hold 277:21 316:4
393:10,11
home 228:20,22,25
229:2 346:23
honestly 323:16
425:20
honor 214:5 216:6
238:13 252:12
253:9 254:1 255:2
255:8,12,20
256:10,17 257:12
258:8,16 259:19
261:22 270:21
275:19,22 277:15
278:2 300:25
305:14,17 309:21
311:5 316:10
317:11,22 319:4
319:21 320:14,21
321:11 322:11,23
324:12 325:1,4,9
325:10,20,24
326:7 327:15,19
328:18,24 330:11
330:12,14,16,20
330:25 331:9
333:6,17 334:9
336:1,5 337:10,14
338:3,8 339:8
342:18,21,23
343:20 344:10,20
345:15,25 346:8
346:11 347:18

348:3,22,24
349:12,21 350:1
350:17,21 351:11
351:16,18,21
352:4,9,10 353:6
353:16,17,24
354:6,16,19 355:2
357:8,16,18
366:11,22,25
367:11,18,23
368:21,25 369:4,5
369:11,15,18,21
370:2,10 371:1
372:18,21 373:3,5
373:7,10,11,21
374:1 375:9,12,19
375:21 376:10,14
376:16 388:9
389:10,15 390:3,6
390:11 392:8,14
393:3,16,20
396:17,20 397:7
399:21 403:18
409:19 414:6,19
414:22 415:14
416:10,16 417:2,9
431:14
Honor's 345:18,21
375:25
HONORABLE
211:12
honorably 332:24
hope 258:6
hordes 373:24
horrible 386:7
hospital 304:17
384:24
hospitals 304:3,11
384:2
hot 256:1 264:12
hotline 380:1
hour 310:11 428:10
hours 257:23 292:14
292:16,17,18
human 223:3
313:14,15,19
hundred 252:23

388:13
hundreds 233:4,5
381:3 386:4
420:22
Huntington 213:4
343:19 344:2,10
346:1,7,11 348:21
351:10,16 352:10
352:14 353:17
354:9,23 355:7
357:2,4,7,11,15,20
366:14,25 367:1
367:24 369:5
370:10
Hyer 253:8 270:25
271:2,4 272:16
273:3
hyphenation 432:22

I

IAPP 387:2
ID 210:15 377:12,14
377:15,17,22
378:8 379:3,9,11
380:10 381:1
382:10 383:20
386:11 411:25,25
412:5 426:9,14
idea 239:3 371:11
388:10,11
identical 350:8
identification 305:7
345:14 346:13
348:6,10,16 350:7
351:3 353:10
354:3 366:18
identified 249:1
318:19 363:1
369:2 386:16
425:8
identify 247:7,18
261:20 308:20
333:24 366:17
378:24 380:7
382:19 383:17
384:4 385:1
387:17 389:5

404:14 405:12,25
421:3 424:13
425:19
identifying 398:23
428:2
identity 212:10
217:3,3 227:11
315:19,19 331:18
333:18,21,23,25
333:25 334:3,6,7
352:24 356:25
366:7,17 367:15
370:9 371:21
378:10,11,25,25
380:6,7,23,24
382:11,12,14,15
382:20,23 383:1,7
383:10,11,14,15
383:21,22,23,25
384:6,7,9,13,14,15
384:19 385:2,4,5
385:10,11,19,20
385:24 386:8,9,12
386:13,17,17
387:7,11,12,18
388:10,19,23
389:20,21 390:16
390:17 391:5,5,19
391:19,23,23
393:18,19 394:12
394:12,14,15,16
394:19,21,23
395:1,4,5,7,8,11
395:14,15,16,21
395:24,25 396:3
396:10,12 399:2,5
400:15,15,25
401:1,11,12,17,17
401:23 402:12
403:1,1,6,6 404:10
405:6,7 406:10
409:9 410:14,15
410:22,22 411:22
411:22 412:2
413:1,25 414:2,12
416:9 417:14,14
418:4,7,7,22,23

419:6,6 420:5,5,11
420:12,17,18,18
421:3,4,7,9,17,24
422:3,16,17,18,25
423:16 424:5,6,8
424:14,23,24
425:1,3,8,10,11,12
425:14 426:3,7
427:15,25 428:6
429:25 430:1
431:4,6
II 212:17
illegal 300:5
illicit 395:12 412:2
  414:4
illness 427:2 428:17
  428:21 429:14,17
illustrative 389:17
imagine 257:23
immediate 291:21
  298:22
impact 230:1 266:12
  290:4 291:7,9
  294:11 298:24
  299:2 300:11
  405:10 424:13
  429:8,9
impersonate 395:5
implement 237:9
  295:18
implementing 251:2
implications 290:25
  292:3 304:13
  428:23
important 250:18
  250:20 251:5,21
  251:23 283:10
  286:13,18 299:12
  299:13 300:16,18
  300:20 301:12,21
  301:21 354:11
  385:6,8
impossible 414:17
in-house 223:19
inability 268:21
  270:1 323:4
inaccurate 365:14

372:9
inadequacies 219:15
  242:1
inadequacy 215:5
  219:12,18 220:2,5
  220:9
inadequate 219:4
  269:1 307:13
inadvertently 223:6
  299:14,23
incident 379:17,19
  380:14 404:14,15
  410:5 416:13
  419:18 428:18
  429:3,14 430:7,17
incidents 404:12,13
  404:16
include 240:11
  309:9 387:1
  390:19 395:2
  405:21 406:5
  419:22 427:1
included 240:19
  272:15 339:24
  340:16 411:11,12
  411:12,13
includes 387:3,5
  394:17 396:4
  408:2
including 294:21
  386:12 390:16
  399:10 404:8
  423:4 428:23
incorporate 364:6
incorporated
  242:22 338:23
incorporates 244:16
incorrectly 372:6
increase 402:1
  425:5
increased 316:25
  317:25 318:22
  319:1,14 322:7,13
independently
  401:3,7
indicate 242:11
  247:5 363:15

364:11 370:9
  403:25 405:23
indicated 214:22
  221:16 229:21
  230:21 232:9
  248:5 249:4,5,6
  278:8,20 283:8
  301:8 323:18
  363:13 408:1
indicates 222:20
  268:23 276:9
  363:23
indicating 216:14
indication 223:23
  328:10 372:13
indications 226:23
  229:13
indicative 371:21
indicia 350:23
  369:16 370:19
indictments 372:5
individual 220:10
  223:2,7 267:13
  273:21 275:6
  286:20 290:24
  299:14 344:4
  346:23 347:1
  361:1 363:15,24
  364:3,20 368:19
  385:1 386:5
  412:15 424:7,18
individual's 300:6
  346:23 395:4
individuals 251:9
  252:24 260:21
  272:19 277:14
  335:4,16 356:17
  356:19 358:4
  361:2,15 363:2,7
  363:20,21 364:10
  367:3 378:24
  379:21 403:14
  406:12 407:5
  422:6
indulgence 326:8
  353:18 390:7
  407:16 410:12

industries 234:20
industry 230:14
  234:14,15,17,18
  234:19,22,24
  238:20 295:12
  309:4 329:9
  388:16,19,20,25
influence 426:13,16
information 217:2,4
  217:8 227:22
  231:8 233:21
  234:21 236:4
  237:10,11,15,21
  238:2,3,8,19,22,25
  239:4,22,24 240:4
  240:10,15,24
  241:15 242:12,23
  243:1,24 244:2,7
  244:14 245:12
  247:22 250:5,12
  250:17 252:17
  253:2 254:20
  260:1,9,14,18,20
  261:14 262:10,15
  262:17,20,22
  263:14,15,17,21
  264:2,3,6,8,17
  265:1,5,10,24,24
  266:3,5,7,10,14,20
  266:23 267:4,7,9
  267:18,24 268:1,8
  268:12,17,25
  269:6,9,12,15,19
  269:24 270:3
  271:16,18 272:4,9
  272:14,20,20,24
  273:7,11,16,18
  274:9,23 275:4
  284:4 292:22
  293:1,12,16
  294:17,24 295:3
  298:14,19,19,20
  299:18,21,22
  300:7,12,19
  302:20,21 305:9
  305:11,12 307:2
  308:4 309:1

312:15,20,23,23
  313:1,24 314:4,10
  314:17,18,23,25
  315:1,2,3,18,20
  316:3 317:1 318:3
  318:10,25 319:18
  323:14,15 326:25
  327:4,12 328:7,22
  329:3,5 335:4,16
  335:20,22,23,23
  335:24 336:21,23
  337:1,12 339:21
  339:24 340:2
  343:13,14 345:3,4
  347:8 359:8
  361:18 362:6,7,8,9
  362:13,18,20,23
  362:25 363:6
  364:7 365:6,9,14
  367:10 368:2,6,15
  371:13 378:17
  380:2 381:18
  384:10,25 387:5
  391:12 392:21
  393:12 394:9,10
  394:19 396:2,6,8
  396:16,21 398:14
  398:17,24 399:4
  400:19,23 401:5,9
  401:21 402:1,3,5
  402:13 403:3,5,11
  404:8,8,20 405:2
  405:19 406:11
  407:6 408:3,6
  409:4,8 410:15,20
  410:24 411:7,8,15
  411:24 412:10,11
  412:13,21 413:2,4
  413:5,10,18,24
  414:1,4,5,7,8,14
  414:16,17,18
  415:22,23 416:1,1
  416:19 417:16,25
  418:1,9 419:9,13
  419:15 420:3,3
  421:1,10 424:16
  424:21,21 425:2

426:22 427:16,17
427:20 428:16
429:1,13 430:6,16
430:24
informed 355:16
infrastructure
235:7 245:7,20
251:7 286:25
292:4,6 308:2
309:16 318:8
initial 329:20
335:10 411:12
initially 283:6
355:23
injuries 394:21
418:25
injury 402:12,16,19
403:13,24 404:1,9
405:6 431:12
inoperable 225:18
225:21
input 343:3 360:4,6
360:20 365:23
inputted 342:10
359:2,19,22 360:6
inputting 343:13
inquire 416:24
insecurity 219:4
insert 409:14
inspection 345:21
installed 283:7
instance 275:16
365:13 399:8
409:22 419:7
instances 346:21
364:14 399:14
419:1
Institute 390:20
423:9,15,24 425:9
431:3
Institute's 391:3
431:4
institution 406:8
institutions 295:12
384:1
instruction 393:7
insurance 218:17

263:23 273:12
300:4 395:18
396:5 399:11
405:22 408:2
411:16,17,17
412:16 413:5
414:5 422:21
427:4,5 430:17,20
intend 257:15
intended 354:21
intentionally 299:21
interact 223:15
382:2
interacting 223:4
interdisciplinary
333:10
International 387:1
390:19 391:10
Internet 223:5,15
227:22 228:8,9,11
228:12,13,15,18
229:5 261:12
262:5 284:11
287:12,14 288:22
289:18 291:6
390:21
interposed 271:19
281:20
interrogatory
260:11 270:2,6,9
270:16 273:6
interrupt 217:13
308:14 325:25
interview 352:20,23
interviewed 304:14
interviews 353:1
intimately 231:13
introduce 223:6
322:17 331:14
377:9
introducing 223:8
intruder 285:13
intrusion 226:2,6,8
281:19,23 282:2,6
282:9,15,17,18
283:18,24 284:1,5
284:11,14,16,18

284:22,23,25
285:9 286:8,10
287:5,6,7,9,13,15
288:2,3,5 312:1,2
312:3
intrusions 311:23
investigate 333:24
investigates 332:6
investigation 341:20
342:4 354:11,25
investigational
274:13
investigations 335:7
investigative 275:25
276:14 335:2
352:18 356:11
investigator 331:17
331:24 333:22
334:19 340:12
352:17 354:4,10
370:17
investigators 335:3
investigatory
334:21
invited 390:23 391:4
involved 265:4,23
266:18 267:3
355:19 381:11,23
382:5 383:9
389:18
involvement 265:8
381:8
involves 379:18
involving 394:8
IP 228:23 416:2,7
416:15
Ironsides 331:1
336:10 373:19
ISP 228:23
issue 260:24 330:5,8
349:18,19 350:2
383:8 400:19
406:25 420:14
issued 216:10
issues 227:3 328:4
329:10 336:25
380:7 382:15,19

383:6,13,17,24
384:4 385:21
386:12,16 391:20
395:6 405:24
424:7
items 419:23

J

January 222:1
Javelin 423:5
job 220:14 258:24
264:2 268:18
269:9,13,17,19
272:25 286:24
335:13 352:21
jobs 250:6,13
252:18 253:3
254:21 260:1,10
261:15 263:11
264:7 272:5,16
273:17,23
Johnson 256:13
257:18,22
joined 389:4
joins 330:16
joint 376:6
jointly 375:17
Josett 211:19
432:16
judge 211:13 214:3
214:6 215:8,11,18
215:25 216:4,15
217:12,19,22
218:6 219:9 228:4
228:6,16,20 229:1
229:4,9,11 238:10
241:17,21 255:3,9
255:13,19,21
256:15,18 257:1,4
257:17,25 258:14
258:18 259:20
261:19 270:6,9,14
270:20 275:21
276:2,6 277:21
278:4 283:15,22
284:7 285:6,11
286:5,13 287:1,11

287:16,22 300:21
301:5 302:4
305:15,19,25
306:7,11,16,25
307:12,21 308:12
308:14 309:2,7,18
309:23 310:2,7,13
311:3 316:4,11
317:4,9,16 319:5,8
319:17,23 320:4
320:12,15,17,22
321:3,6,10,14
322:12 324:10,14
325:2,6,11,13,17
326:2,9,12 327:13
327:16,24 328:16
328:25 329:11,13
330:13,22 331:1
331:10 333:4
336:6 337:3,16,18
338:7 339:5
342:14,17 343:24
344:8,11,17
345:13,23 346:5,9
346:12 347:11,22
348:25 349:5,15
349:22 350:3,19
351:9,14,17,19
352:1,5 353:12,21
354:7,12,17,20
355:4 357:13,19
366:20,23 367:19
368:23 369:3,9,12
369:24 370:24
371:2 372:19
373:2,4,9,14,16,22
375:2,7,11,22
376:4,12,15,20,24
379:11 384:5
387:21 388:1,7
389:8,24 390:4,9
392:13,16,20
393:1,4,21 394:1
396:22 397:2,22
398:18 399:17,23
399:24,25 409:10
409:13,25 410:7

412:5 415:3,7,9,15
416:11,21 417:6
419:2 422:12
428:8,11 431:17
431:19
judgments 335:24
judicial 364:8
July 222:1 236:22
236:23,24 324:24
362:2
June 236:22 289:6
332:25 341:11
408:23
jury 329:14
Justice 423:5
JX 210:22 375:14,18
375:20 376:8

K

K-A-M 377:10
Kaiser 389:2
Kaloustian 274:14
274:18,23 275:14
277:2,3,6,10 278:9
278:21 279:7
Kaloustian's 275:24
276:13,23 278:13
Kam 210:12 370:8
375:10 376:17,19
377:3,8,10 378:8
378:14 387:25
388:6 389:18
390:7,14 392:18
393:10,17 394:7
394:14 395:14
397:9 398:2,8,22
400:11 403:8,21
404:11 407:7,16
407:18,22 409:11
409:20,23 410:3
410:11,14 412:9
414:25 415:18
416:16 417:11
421:8,23 423:25
426:9,17 427:6,10
427:13 428:15
430:5

Kam's 396:21
414:21
keep 240:12 242:15
243:4,10,18 257:6
257:20 279:24
307:5 339:5
359:10 373:9
keeping 307:8
keeps 255:23
KENT 213:4
kent.huntington...
213:12
kept 294:2
Kevin 330:15 331:6
331:16
key 386:16
keystrokes 365:24
kind 214:18 255:25
308:18,25 383:12
400:19
kinds 339:24
knew 233:16 234:8
302:14 420:20
know 215:12,21
216:13 218:14,24
220:5 222:13,14
228:11 229:7
231:3 234:10
237:24 238:4
240:23 241:2,13
245:2,10,21 255:4
255:5 256:22
258:3,23 262:13
269:18 279:8,12
279:15,19,20
281:22 286:4,12
297:15,19 299:20
302:13,16,18,19
302:20,23 308:5
320:5 323:6
330:24 336:13,23
337:11 339:10
340:20 341:1
344:3,5 355:12,22
356:25 357:21
358:9 364:2,22
365:5,11,15,18

366:5 367:20,25
368:4,9,13 371:21
371:23 376:22
383:3,4 385:8,22
385:23 386:3
388:9 390:18
391:9 392:2
396:14 398:12,16
399:3 401:13
402:22 406:20,22
412:13,17 415:11
415:15,24 416:13
417:17 420:7,20
421:5 422:24
424:2,25 429:8
knowing 220:1
400:18 401:3,7
417:18 419:8
knowingly 367:9
368:1
knowledge 230:18
234:4 252:2
254:19,22 301:17
314:6,7,9 326:14
326:21 328:3,6
343:21 344:6
367:17 388:18
416:13,14 432:10
known 237:22
238:20 247:8,18
332:3 366:7
knows 216:16
228:23 339:6

L

lab 262:11,22 263:2
263:22 271:15,17
272:15,21 273:8
273:11 302:15
lab-related 263:16
labeled 311:12
397:15
LabMD 210:3 211:4
218:18 219:5,12
220:20 222:5,10
224:2 226:13,15
227:2 228:7 229:4

229:17 230:8
231:23 247:7,17
248:11,14 252:23
253:1,15 254:20
260:8,12,16,17,21
261:12,25 262:9
263:10 265:8
268:21 269:5
271:6 272:4,8
275:1 278:8 279:4
279:9,15 280:25
282:21 283:13
284:21 288:1,25
289:9,18,22
292:12 293:18,22
294:7,17 295:5
296:7 297:18,23
298:14,17,25
302:8,9,19,24
304:3 312:11
313:5 316:1
318:14 338:23
342:4 344:5,7
350:25 354:11
355:1,25 356:3,4,5
356:10 358:6
359:8,18 397:20
403:15 405:2,11
408:7 417:23
420:1 430:25
432:4
LabMD's 214:23
215:5 219:3,13,15
219:18,18,22,25
220:3,6,18,22
221:2,17 225:7
227:20,22,25
228:1 229:22
230:14 232:20
234:5 237:25
241:25 248:6
260:14 270:1
279:25 285:2
288:10 293:3,24
293:25 294:1
312:24 313:5
316:23 318:8

319:15 322:8
323:5,15 403:9
404:6,18,25
laboratories 304:3
laboratory 263:4
265:4,9,24 266:18
267:4,6,12,17,25
268:8,24 269:4,14
399:12
labs 384:24
lack 215:5 247:22
307:19
lacked 327:10
lacking 371:8,15
laid 295:9
LAN 229:5
language 241:24
lap 298:1
lapsed 422:21
large 243:21,22
249:16 296:3
307:6,9
largest 388:14
Lassack 212:6
253:20,25 277:15
278:2 305:17
310:11 311:5,8
316:9,14,16
317:11,22,23
319:3 320:1,9,14
320:16 323:9
324:12,17,25
325:25 327:15,19
328:1,24 329:1,12
330:12
late 256:5 257:19
388:11
latitude 353:19,25
LAURA 212:4
law 211:13 330:20
330:22 332:15
333:15 342:11,17
342:19 372:4
416:8
Lawrence 377:3,10
laws 323:20 400:21
lay 317:17 345:16

349:12 354:14
367:17,18 396:23
397:22
layers 308:9
leading 277:20
learned 306:22
leave 255:25 312:17
333:15 351:24
leaving 264:9
283:20
led 424:9
leeway 297:19
left 220:22 221:2
285:2,3 312:11,21
338:4 340:6
legal 231:10,12
394:4 422:18
legally 363:15
legislators 386:20
lenient 255:9
let's 221:12 226:19
253:8 255:10
280:14 287:4
292:7 327:24,25
334:18 354:17
357:1 373:9 390:1
403:19 411:4
415:18 428:4,4
letter 291:5 294:14
294:23 313:10,12
313:20 401:15
420:9
letters 379:23,24
letting 255:10
level 249:15 318:22
381:8 403:25
levels 266:5 273:7
309:15
liaison 334:1 381:10
381:14 382:1
licenses 332:5
lies 380:4
life 412:22 413:13
413:16,21 414:15
light 398:11
likelihood 218:10
370:23

LimeWire 220:13
280:17,25 281:10
284:20 287:25
288:5
limit 243:15,19,19
253:4 257:21
268:20 269:10,21
273:24,25 274:2
287:20 354:17
limitation 268:15
423:25 431:8
limitations 269:3
296:14
limited 261:13
262:17,23,25
263:10 268:2,13
268:24 269:2
272:4 292:15
316:6 317:20
322:20 353:13
382:17 383:16
limiting 245:18
266:13
line 215:9 238:15
254:19 262:2,3
264:14,23,24
271:12 279:23
280:11 281:17,21
320:5,7 343:1,2,12
343:12 359:18,18
431:16
lingo 305:22
link 290:12,18 294:9
356:25
list 242:21 354:21
386:24,24
listed 233:14 328:13
341:24 356:16
360:5 367:25
368:4,19 392:16
listen 385:16
lists 308:5
literally 381:3 386:3
388:13 425:18
literature 239:6
240:16,25 306:19
403:4 418:24

litigation 216:10
342:5
little 222:25 223:10
264:10 296:5
389:8 399:22
402:4
live 412:22
LLP 212:19
loan 366:1
local 228:14,17
379:5
located 215:22
locations 271:22
409:5
Lockers 293:22
locks 293:5
lodge 277:16
logged 248:15 285:1
logs 227:25 228:2
230:10 248:3,7,7
248:16 249:4,9
285:1 312:10,22
323:13,18,20,21
324:1,4,7
long 214:17 236:25
304:24 306:12
331:19 332:8
336:13 377:22
393:14 412:21
413:13,15,21
414:15 417:2
longer 224:22
257:23
look 230:24 231:3
237:5,7,18 244:13
245:1,4 247:20
249:23 259:13
261:9 264:13
271:11 274:6
276:24 277:8,14
288:17 289:4
293:17 303:14
304:4 307:1
308:18,19 321:4
326:23 336:17
383:7 397:9 398:4
404:17 405:9

410:9,15 422:22
424:17 425:17
looked 230:13,21
233:7,15 247:22
288:10 304:1,11
372:8,10 407:11
418:22 422:24
423:3,21 424:2
425:13
looking 216:6 233:7
233:10 243:23
320:21 359:17
380:17 383:5
385:15 399:15
400:12 403:21
405:18,20,25
418:12 425:1
looks 273:18 375:2
lose 430:16
losing 430:20
loss 427:4
losses 422:5
lost 368:14 420:22
lot 295:2 305:21
382:15 410:1
love 420:20
lunch 288:24 305:18
310:8,16
lvandruff@ftc.gov
212:14
Lytec 314:17

M

M 432:25
M-E-H-M 373:15
ma'am 302:11
machine 222:15,16
223:1,2,6,7,8
226:5 227:13,14
227:15
machines 224:6
Madness 286:6
mail 288:17 368:10
401:15
mailing 379:23
main 276:25
maintain 237:9

maintained 252:23
260:21 292:5
293:25 294:7
317:1 318:25
348:11 405:2
maintaining 243:22
251:10 278:25
279:3
maintains 396:16
398:14,17
maintenance 277:6
Maire 253:12,14
254:6 261:2,20,24
265:16 277:10
278:8
Maire's 253:19
261:5 265:22
266:11
major 243:12
362:18
majority 296:12
making 284:4 344:6
380:21 381:23
malicious 226:2,5,7
286:11,17,22
287:4,8 288:7
malware 248:1
management 307:6
378:3 381:10
387:5 391:12
management-app...
261:13
managers 262:4
manner 318:10
manual 313:5
map 250:25
Marbury 332:15
March 286:6 327:23
341:10 388:20,21
MARGARET 212:6
mark 331:21
marked 338:13
348:6,10,15 350:6
351:2 353:10
354:2 366:18
427:7
market 413:6,9,11

Maryland 332:2,6,9
  332:10,13,16
  334:2,4
mask 395:5
matches 347:9
matter 211:3 327:20
  334:12 356:4
  360:14 370:22
  375:10 397:20
matters 333:25
  334:6 335:13
  337:11
mean 217:15 218:3
  225:18,20 226:1
  234:15 256:20
  270:6,9,17,19
  276:16 281:22
  282:4 299:4
  306:11 308:14
  312:14 314:15
  330:4 365:22
  366:9 378:19
  382:13 402:18
  425:22
meaning 262:15
  317:18 336:20
  409:2
measures 247:7,18
  250:4,11 252:16
  259:24 260:8
  277:12 279:24
  280:3
mechanism 299:10
  299:12
mechanisms 235:4
  240:7,8 250:23
  269:21 287:20
  290:19 295:19
  297:5,6,11,14
  304:18 306:6
  307:20 308:1,2,5,8
  308:20,24 309:15
  312:18 313:18
media 381:11 392:4
Medicaid 395:19
  414:8,11
medical 217:3 231:9

234:24 235:3,12
  246:11 303:2,3
  304:2,6 315:19
  328:20,23 329:3,5
  329:6 367:10
  368:6,15 378:11
  378:25 380:24
  382:12 383:10,15
  383:21,22,25
  384:6,19,21 385:2
  385:5,11,20 386:9
  386:12,17 387:7
  387:11,12,18,19
  388:10,23,23
  389:20 390:16
  391:5,19,23
  393:18 394:12
  395:8,14,15,16,21
  395:24,25 396:3,9
  399:5,6,12 400:15
  401:1,11,17
  402:12 403:1,6
  404:8 405:7,23
  410:15,22 411:13
  411:22,25 412:5,6
  412:20 414:11
  417:14 418:7,23
  419:6 420:5,12,18
  421:2,4,8,17,24
  422:3,20,25
  423:16 424:6,8,14
  424:24 425:2,8,11
  425:11,14 426:2,7
  426:25 427:14,25
  429:2,7,23,24
  430:22 431:4,6
medical-related
  246:15
Medicare 395:18
  414:8,11
meet 293:11,14
  307:14,16,22,25
  394:3
meeting 295:6 296:9
  309:12
meetings 391:7,9
Mehm 212:7 373:11

373:12,15,15,21
  374:1 376:16,21
  377:7 387:24
  389:15 390:3,6,11
  390:13 392:14,18
  392:25 393:3,6,8
  393:16 394:6
  396:20 397:1,6,8
  398:1,21 399:21
  400:9,10 409:18
  410:2,8 412:8
  414:19 415:6,8,14
  415:16,17 416:16
  417:9,10 419:3,4
  428:10,13 431:14
  431:18
member 386:23
members 368:5
memory 238:5
mention 258:19
  411:16
mentioned 385:9
  391:13 414:2,6
  417:17 424:20
  428:1 429:22
merely 300:23 339:6
merge 429:25
merit 409:17
met 230:15 370:20
method 407:20
methodology 327:11
  327:22 393:23
  404:22 407:19
  409:19 425:19,22
methods 298:15
Michael 211:12
  213:6 417:21
microphone 327:18
  331:3 346:10
middle 372:11
  411:11
MIFA 387:7,10,15
  387:16,20 388:8
  389:8,11,11
military 306:4
  332:18
mine 338:4

minimum 424:4,4
  425:25
minor 324:12
minute 217:13
minutes 310:12
  425:23 428:12
mischaracterizes
  359:1,22
misconfigurations
  313:17
misdiagnosed
  428:17,21 429:18
misdiagnosis 427:1
misled 329:15
misrepresentation
  375:21
missed 354:13 393:7
misspoke 315:8
misstated 236:14,17
  277:24 278:3
misstating 221:15
mistake 313:19
mistaken 375:16
mistreated 429:14
mistreatment 427:2
  429:20,21
misunderstanding
  313:16
misuse 421:7
mitigate 419:10
mitigated 417:13
  418:6 419:6
mitigation 406:13
  417:12
model 243:13
moment 252:11
  255:13 260:4
  275:16 302:2
  334:18 387:9
  402:7
momentarily 409:23
moments 283:17
  323:10 334:9
  411:6
money 307:9 338:21
  358:14
monitors 421:5

month 224:22,25
  324:22 331:21
  391:15,21
monthly 392:2
MORGAN 213:5
  389:10 392:8
  393:20,22 396:17
  416:10,12 417:2
morning 214:15,16
  255:10 311:14,22
  312:9 313:4,10,22
  315:11
motion 327:19
  375:18,23 376:1,5
motivation 367:15
move 319:19,21
  349:13 357:1
  369:6 373:22
  390:1 409:20
moved 271:21
moves 350:22
moving 250:2
  412:18
multiple 222:17
  245:4 275:11
  285:25 296:14
  308:9 363:2
  412:18

_____ N _____

N 210:2 214:1 311:1
  311:1,1 432:1,19
N.W 211:15 212:11
  212:20 213:8
name 260:12 331:16
  347:9 357:23
  363:8,21 366:7
  372:11,11,12
  373:14 377:10
  394:17 396:4
  405:21 408:1
  411:11,11,11
  412:16 419:15
named 246:1,22,23
  256:9
names 340:1 341:18
  341:24 342:2,9

345:9 346:20
347:7 348:18
350:14,15 356:15
356:17,22 361:4
361:15,17 363:5
363:10 365:4
370:7 372:10
411:11
National 235:2,11
246:10,24 389:3
390:20 391:2
nature 381:20
405:18 411:6
necessarily 226:8
228:12 290:24
421:1 424:15
425:1
necessary 272:5
328:21 330:7
401:16 425:7
need 217:24 240:12
242:16 243:5,10
243:15,18,19
251:13,14 254:21
258:14 259:1,4,7
259:12,12 264:6
267:11,12 268:18
270:14 273:24
291:2 293:1
294:16 296:18,21
296:23 297:7,9
304:7 307:5 308:7
308:8 310:9
316:13 317:16,17
317:18 321:3
329:17 330:23
336:20 346:9
376:4 392:20,23
396:23 397:22,24
428:9
needed 220:14
250:5,13 252:17
253:3 260:1,10
263:21,24 264:1
267:13 269:13,13
269:19 272:24
273:9,11,16,22

284:2 307:7
314:23 329:23
388:24
needing 292:18
needs 251:24 258:5
negative 230:1
382:21 430:14
network 221:18
222:5,11,23
227:12,21 228:1,1
228:14,17,24,25
229:23 247:9
248:6,18 249:2
260:14 271:15
279:25 282:18,22
285:2,4,8 286:19
308:9 310:4 312:4
312:17,19,21,25
317:1 404:21
408:15 409:3
networks 247:20
295:20 318:11
405:3 410:16
never 224:8,11
252:24 260:22
273:2 276:10
385:24
new 251:12,15
322:17 395:1
414:3
news 392:9
nine-digit 340:11
344:3 356:16,18
359:19,23 360:9
360:12,17,20
361:1 405:21
411:13
NIST 232:14,17,18
232:19,23 233:7
235:10
nonpublic 362:8
normal 223:13
292:14,16
notations 340:24,25
341:2
note 255:21
noted 360:15

notes 432:8
notice 327:21 376:5
376:6 419:10,12
420:1
notification 378:23
379:23,25 400:13
400:21 401:2,10
417:23 419:22
420:9
notified 401:14,21
417:19
notify 400:22
notifying 378:17
notion 238:6 275:2
293:16
November 408:21
408:25
number 253:21,23
254:3 273:20,25
320:5,7,7 343:3,6
344:3 345:9,10
346:21,25 347:9
359:23 363:9,11
363:16,18,19,25
364:4,12,13,17,18
369:10 371:22,23
372:7 394:18
396:5,5 405:25
412:19 413:7,8,13
419:16 424:4
426:1,1,2 427:24
428:2 432:3
numbers 340:3,4,5
340:7,8,11,11,13
340:15,16,19
341:17,23 342:1,8
342:10,12 343:1,8
343:21,22 344:1
344:13,23 346:19
347:7 348:17
350:10 351:7
356:14,16,19,20
356:22 357:22
358:2,3,7 359:2,11
359:19 360:4,6,7,8
360:9,10,11,12,15
360:16,20 361:1,3

361:19 363:3,5,11
364:9 365:2,23
367:4 370:3,6
371:19 405:22,22
411:13,17,18
412:25 413:5

O

O 214:1 311:1,1,1
432:1,1,1,19,19,19
432:19
object 257:1 321:12
346:1,2 355:5
389:10 393:20
objected 349:8
objecting 416:25
objection 257:13
271:19 277:16,23
281:20 317:3,17
321:10 322:10
325:20 326:9
327:14 329:25
330:1,10 337:14
343:19,24 345:24
346:12 348:21,24
349:5 351:1,1,10
353:6,13 354:8
355:2 366:10,21
367:11,19 368:21
370:11 389:24
390:4 392:8,22
394:1 396:17,22
397:3,25 398:19
400:4 416:10
417:1,5
objections 369:6
objective 424:13
425:20
observation 348:20
349:2
observations 348:14
349:17
observed 341:9
observing 341:11
obtain 335:4 355:20
367:2
obtained 355:23

obtains 362:18
obvious 299:3
321:19
occur 217:8,14
218:2 223:12
225:6,14 226:8,10
226:11 251:6
272:23 286:10
287:7,10 288:3,5
301:18 382:15
386:8 395:9
occurred 217:6,10
226:24 227:17
230:8 280:17
281:2,3 312:16
359:1 400:23
occurrence 224:25
occurring 284:6
occurs 223:11,13
October 387:14,23
388:9
offend 299:4
offer 242:6 317:24
352:6 420:16
offering 369:10,25
office 288:22,25
289:22 293:23,24
334:4 375:14,25
376:2 399:9
officer 331:2 373:20
380:17
offices 302:15 304:3
official 388:8
officially 388:2
oh 217:21 218:5
281:8 286:20
323:20,21 325:4,9
375:22 411:16
okay 214:21 215:18
217:21 218:17,24
222:13 224:24
225:17 226:7
231:6,16 241:21
247:17 248:19
249:22 250:16
253:7 254:15,25
255:3 260:23

261:4 266:16
275:18 276:2
278:12 279:21
280:10,13 281:8
282:20 284:7,15
286:13 287:22
288:16 289:12,16
290:1 293:21
301:4 303:18
304:8 308:16
310:7,13 316:9,14
323:20,22 324:4,8
325:16 326:5
328:16 337:1,16
344:8 347:17
350:5 352:1
353:12 369:9
373:16 376:15
397:1 415:3,9,16
on-the-ground
    385:19
once 276:13 282:21
    294:22 331:3
    380:14 383:12
    391:21 407:1,5,5
ones 313:9 391:1
ongoing 303:23
    413:23 414:13
online 229:6,9
open 283:20
opening 288:2
opens 287:3 288:4
operable 294:2
operating 279:16
    303:24
operations 298:15
    300:9 304:1,4
    378:4
opinion 218:10,12
    219:22,24 222:1
    226:21 231:17,23
    232:11 236:1,8
    239:7 240:16
    243:5 247:6
    248:22 260:19,24
    263:9 264:21
    266:13 272:3

274:18 275:15
284:20,24 285:7
287:12 293:3
295:6 296:8 301:1
307:12 309:19
310:2 313:8
316:23 317:7,9,19
317:24 318:6,7,16
318:17 320:11
321:18,23 322:1
322:18 326:22,24
329:15,19,19,22
330:3 366:12
367:15 396:23
397:4 400:7 403:8
403:12 404:4,6
409:15 410:21
opinions 230:18
    236:17 242:7
    258:25 298:7
    311:18 317:20
    322:19,19,20
    324:23 327:21
    341:19 389:22
    390:2 394:3
    399:19 400:2
    410:1
opportunity 256:24
    284:13,17 285:22
    287:7 351:5
    376:18 386:14,18
    397:3 400:24
    418:1,21
opposed 424:6,19
opposing 327:13
option 301:3
order 245:11 251:13
    252:20 253:3
    256:16 263:10,22
    264:6 268:18
    272:15 273:11
    296:18,25,25
    297:17 304:3,15
    304:17 305:8
    308:3,10 336:8,19
    337:3,9 338:21
    342:25 358:14

385:4 406:14
orders 337:13
Oregon 377:16
organization 264:7
    269:18,24 291:18
    295:15 312:8
    315:5 327:8
    378:15,22 379:18
    380:12,18,19
    381:16,19 382:4
    387:22 388:12
    391:13 394:7
    400:18 417:18,19
    419:12,21 420:10
    420:15
organization's
    240:5 292:4 401:4
    401:7
organizations
    243:12,22 293:15
    296:2,3,3 307:8
    379:2,6,6,7 384:25
    387:13,17 389:1
    390:15 399:10
    400:21 406:20,23
    420:22 421:1
    423:4
originally 298:4
    306:3
originates 312:4
out-of-pocket
    421:22 422:5,7,10
    422:12 424:10
    426:6,7 431:11
outcomes 380:21
output 347:3
outreach 334:6
outside 226:2,5,8
    248:7 255:24
    256:2 257:21
    282:10,17 287:16
    287:18 312:4
    330:17 396:18
outweigh 272:7
outweighs 351:13
    370:18
overall 245:23

250:24 263:16
264:21 272:14
285:18 290:12
291:2,17 292:3
294:11 410:18,21
429:10
overlap 267:9,12,16
overruled 277:23
    330:10 390:4,5
    394:1 398:20
overview 233:8,16
Owens 338:15
    345:11 357:5,10
    427:8

P

P 214:1 432:1,19
p.m 257:21,21
    310:14,16 311:2
    375:4 431:23
P2P 404:14,24
    407:24 410:5
    418:16,16
page 216:19,22
    239:11,17 247:1
    249:21,23 252:15
    253:7,8,18 254:8,9
    254:18,25 259:24
    261:6,10 262:2
    264:13,23,23
    266:16,19 271:11
    274:3,7 276:8
    279:21 280:11,12
    280:15 281:15
    289:5 292:7,8
    293:17 298:2,3,5
    298:10 300:2,3
    311:13,16,16
    320:5,7 338:21,22
    339:25 340:8,21
    340:22,23 341:3
    343:2 357:1,12
    363:22 398:2,5
    399:15 400:11
    403:20,23 404:3
pages 233:4,6
    338:20 339:22,25

340:6,23
Pam 423:1
paper-based 399:6
papers 386:19
paragraph 216:23
    236:11 237:7
    239:19 240:12
    241:24 247:5
    249:23,24 252:16
    274:7 276:9
    277:19 288:21
    291:11,19 294:16
    309:7 311:12,15
    315:7,9,12,16
    316:20 320:7,9,10
    320:10 398:9
paragraphs 291:11
    311:19 320:23
    321:14,17,23
    400:13
paralegal 332:15
part 224:20 231:7
    232:5 233:8
    243:12 281:5
    282:12 288:17
    292:25 298:6
    304:10,20,23
    313:15,19 322:15
    352:5,20 354:11
    356:10 365:8
    366:3 378:4
    380:16 390:5
    407:18 419:1
    420:23 421:2
participants 399:7
participate 386:15
    390:23
participated 286:2
particular 220:12
    222:16 232:21
    260:24 262:12
    272:25 275:16
    290:6 300:1
    307:10 336:23
    364:12,17 378:23
    379:16 380:14
    386:21 391:16

405:10 409:22
412:14 426:11
particularly 402:12
parties 285:25
375:13,14
partly 420:24
party 337:8
passed 352:3
password 245:15
passwords 295:17
pasted 359:23
patch 240:13 242:16
patching 245:14
patently 322:17
patient 304:14
405:24
patients 358:8
Pause 216:12
252:13 253:10
255:1,15 302:5
303:16 319:16
320:18 375:1
397:17 407:17
410:13
pay 422:20
payers 384:2,24
paying 422:15,15
payment 300:8
413:7
peer-to-peer 280:9
280:17 283:19
285:12 286:14
408:15 409:3
410:16
penetrate 248:18
penetration 248:9
248:15,25 249:5,6
276:9,17,22
277:11 297:10
penicillin 430:13,13
Pennsylvania
211:15 212:11,20
213:8
people 223:18
255:23 266:6,22
267:6,12,14,16,18
267:23,25 268:7

336:7,18 341:17
342:2,9 343:22
345:9 348:18
356:14 361:4
363:5 365:3,24
367:7,25 368:4,9
368:13 370:7
377:17 379:16
380:6,15,23
382:18 383:3
385:9,15 386:1,6
424:5,20
PEPSON 213:6
percent 365:12,19
percentage 425:6
perform 250:5
252:18 260:1,10
263:11 268:18
269:9,19 272:5,15
272:25 286:24
314:7 333:20
341:12 343:7
352:17 367:13
performance 298:20
performed 222:18
224:4,19,21
263:25 267:14
269:18 273:12
297:4 334:13
342:3 348:15
353:9 354:1,10
370:16 382:25
performs 314:6
354:4
period 221:23,25
222:6,11 224:3,12
224:16,18,25
243:7,9 246:13,18
253:15 260:13
276:22 277:1,9,13
279:17 288:24
302:10 303:4
311:20 318:21
323:1 324:5,19,22
332:22 412:22
periodically 297:4
Permanente 389:2

permission 263:1
394:16 395:11
414:25
person 248:17
285:15 300:6
364:11,16 395:15
person's 394:16
395:10 399:11
414:3
personal 237:11
250:5,12 252:17
259:25 260:9
266:9,13,23
267:24 268:1
274:9,22 275:3
288:17,22 289:19
316:2,25 318:10
349:2 361:18
367:9 368:2,6,15
378:16 381:17,18
396:16 398:14,17
401:8 402:1 403:3
403:11 404:8
405:2 407:6 408:3
410:24 416:12,14
417:15,25 418:8
419:9 420:3,21
personally 358:25
362:4 372:8 381:5
persons 262:16
265:3,8,23 266:18
267:3 369:1
perspective 312:6,7
385:23 423:23
pertains 393:24
pervasive 235:9,14
Ph.D 214:9
PHI 300:7
philosophy 333:12
phone 288:18
291:20 353:2
411:18
phrase 237:14,17,20
237:23 238:22,25
239:5,6 241:14
306:8
phrasing 240:22

244:7,9
physical 240:13
242:17 292:24
293:2,4,6,7 345:21
physician 302:21,23
332:4
physicians 332:3,6,9
332:10,13,14
piece 284:1 285:3
pieces 391:22 392:1
pinpoint 425:4
Piper 332:15
place 248:12,15,21
248:23 269:21
279:16,24 280:3
287:20 292:23
294:5 296:1,8
297:21,23 312:18
314:10,24 315:4
387:14 400:20
406:14 412:18
placed 318:10
places 245:4
plain 217:22
plan 233:21 240:5
241:17 243:1,25
251:4,15 258:7
290:17 293:16
296:15,18 300:19
308:5,17 313:16
326:25 327:4,12
379:19 414:24
plane 346:6,8
planning 407:1
play 231:22 381:9
426:9
plays 400:14
pleadings 336:24
please 216:24 219:8
220:8 232:2
239:13,17 240:3
247:2 254:11
260:4 279:22
288:14,15 298:3
303:15 312:13
318:5 320:13
331:14 336:11

338:17 339:23
345:12 354:18
377:9 379:10
384:5 395:23
397:9 398:2,4,8
404:22 406:3
422:11 423:13
427:8
PNC 365:25
point 224:24 250:2
319:13 322:6
381:4
pointed 248:24
police 339:13
355:14,17,22
358:12,17,21,22
370:5
policies 240:6,8,9,13
242:16 245:16
247:24 250:22,24
265:17,18,20,21
283:9 287:19
289:13 290:17
294:8 297:23
300:16 301:17
307:19 308:2,6
313:5,9
policy 251:21,23
252:3,4,6,8,8
265:25 286:5
288:23 289:15,18
289:21 290:3,6,9
290:14,18,19,22
290:23,25 291:1,5
291:8,13,15,25
292:23 294:5,11
294:22 298:23
299:1,5,8,9,15,20
300:10 313:17,20
Ponemon 423:9,15
423:24 424:1,9,12
425:9,13,17
426:10 431:3,4,6
populate 362:13
364:6
populated 361:11
366:8

population 425:15
Portability 300:4
portion 231:19
    232:19 278:19
    293:10
Portland 377:16
ports 240:13 242:16
    245:15
pose 325:20
position 251:9
    261:21
positive 291:7,9
    298:24 299:2
    300:11 380:21
possession 219:3,12
    219:18,23,25
    220:18,22 221:2
    294:19 323:5,15
possibilities 379:15
possibility 284:22
    284:24 287:13,15
    288:2,2,4
possible 223:12
    254:17 314:8,12
    339:7 371:21
    396:14 398:6,12
    398:22
possibly 277:10
    281:24 312:20
    343:25 346:24
potential 298:16
    367:15 382:7
    383:13 400:14
    418:25 419:10
    421:7 427:3
    428:20,23 429:5
    429:16 430:9,19
    431:12
potentially 412:3
    429:10
power 286:4 382:17
    383:17
PR 381:12
practical 385:6
practices 232:22
    240:9 304:5 309:9
    319:15 322:8

354:25 387:18
388:15 396:15
398:13,16
prejudice 351:4
    369:19
prejudicial 351:12
    370:18 371:16
preliminary 334:12
    375:10 402:8
premarked 397:10
prematurely 256:24
premises 294:18
prepared 255:6
preparing 237:3
    402:10,20
prescribe 419:17
prescribed 427:3
    430:7,10,13 431:2
prescription 395:17
prescriptions 427:3
presence 282:22
    325:14 337:15
present 222:19
    243:3,4 249:2
    285:22 318:8,21
    318:23 345:20
    391:4
presentation 290:9
    290:20
presented 256:14
    391:8,9
presenting 391:15
presents 284:13
    287:7 328:10
preserve 372:23
president 377:14
pretend 256:22
pretheft 379:1 380:8
    383:18 385:3,17
prevent 250:4,12
    252:16 259:25
    260:9 282:1
    313:19
prevented 280:4
previous 303:9
    322:14 358:1
    393:5

previously 214:11
    230:10 237:23
    244:19 284:25
    290:16 292:1
    294:8,13 299:9
    317:19 332:3
    414:23 415:1
primarily 333:24
    402:3 406:17
    426:24
principle 243:10
    292:24 307:7,10
principles 236:3
    240:11 242:12,15
    242:21,22,24,25
    243:3,24 244:3,6,8
    244:11,14,17
    245:2,5,6,24 246:9
    293:11,14 295:4
    306:16,20,21
    307:23,25 309:9
    309:11,15 327:5
    329:6,8
printed 349:23
printing 379:23
prior 236:8 243:7,8
    246:12 265:12
    277:17,19 304:21
    311:21 331:23
    332:1,12,14 357:8
    373:8 388:7,9
    400:8
privacy 212:10
    304:12 331:18
    333:18,21,23
    380:17 386:12,15
    387:2 390:16
    391:10,19 393:12
    406:19 407:3
private 217:4
    303:13 315:20
    395:18 414:18
probability 249:16
probably 240:22
    243:17 310:11
    359:22 391:21
    403:24 423:3

probative 351:13
    354:5 370:19
probe 240:13
    242:16
problem 273:13,15
    389:6 414:9
problems 383:9
procedure 256:22
    327:24
proceed 214:6 331:9
    428:12
proceeding 317:21
proceedings 216:12
    252:13 253:10
    255:1,15 302:5
    303:16 319:16
    320:18 337:20
    338:1 375:1 394:3
    397:17 407:17
    410:13
process 233:23
    251:3 304:16
    308:18,18 336:16
    343:11 361:5,8
    369:20 380:19,21
processes 314:24,25
    315:4
Proctor 331:2
    336:10 373:20
procuring 412:6
product 283:19
    334:24 359:5
production 351:6
products 298:16
profession 240:1
    407:9
professional 243:23
    251:18 271:5
    390:14 393:9,12
professionals
    234:11,21 251:1
    269:14,15 276:25
    277:1 301:13
    387:2 391:10
    406:19 407:3
professor 214:15,17
    214:22 215:21

216:6,9,19 217:5
218:13 221:5
232:9 236:7
239:15,18 240:14
241:23 253:11
256:11 259:23
276:8 277:19
283:8 284:9
289:12 292:10
294:4,22 295:2
298:3,4,23 299:7
300:10,15 301:1,3
301:20 303:8,19
305:13 311:9,22
312:9 313:4,22
315:6,25 316:17
317:6,13,24
319:12 322:5,25
324:18 325:5
327:21 328:5,10
328:12,19 329:2
proffered 353:14
    354:9
program 220:19
    237:10,15,21
    238:1,2,4,7,7,9,19
    238:23,25 239:4,9
    239:22,24 240:4
    240:10,15,24
    241:15 242:13,23
    243:25 244:2,8,15
    245:12 250:18
    251:2 280:1
    281:11,12 282:24
    283:23 293:1,12
    295:3 309:1
    326:23 390:22
programmable
    305:10
prohibited 288:23
    289:18 294:20
project 361:24
    362:2 370:16,22
projected 427:24
    428:17
projections 425:23
    430:23 431:9

projects 391:3
proof 269:1
proofread 432:21
proper 294:18 376:9
  394:4 419:12,22
property 288:25
  289:22 293:18,22
  293:25 294:7,17
  294:24
proposed 304:18
proposition 274:21
  275:14
prostate 413:19
protect 235:7
  237:10 240:13
  242:16 243:15
  244:22 245:6,19
  252:5 291:1 316:2
protected 251:8
  281:25 300:7,12
  302:19 328:22
protecting 235:3
  244:25 246:10
  293:8 329:5
protection 212:9,10
  235:4 328:21
  329:3 331:17,18
  333:18,21,24,25
  422:18
protective 336:8,19
  337:3,9
prove 227:11
provide 235:2
  244:24 247:6
  250:25 251:2
  303:23 316:1,24
  338:6 360:15
  362:24 378:9
  379:12 382:6
  384:5 389:5,18
  403:9 404:6,18,25
provided 233:11,19
  252:25 260:22
  292:25 302:9,14
  306:24 314:11,17
  314:18,20 317:19
  318:14,18 328:23

335:11 339:4,14
339:17,19 345:6,7
346:17,20 355:9
359:24 396:18
402:23 411:3
420:1 422:17
425:19
provider 223:20
  344:5 399:13
  412:16
providers 231:9
  234:25 303:2
  422:16
provides 251:7,8,16
  379:20 382:17
  419:13
providing 245:17
  293:5 367:14
  378:23 379:22
ProviDyn 221:6
  226:19,20,24
  229:14 248:10
  249:1,5
provision 379:24
pseudo 329:16
public 210:5 211:10
  335:23 362:7,8,23
  364:8 373:22
  395:18
publication 392:9
publications 392:5
  392:10,16
publish 386:18
published 241:1
  391:22 392:1,7
  406:23 423:1
pull 232:1 427:8
pulled 253:18
punctuation 432:22
purports 253:22
purpose 354:13
  369:25
purposes 217:1
  257:6 294:3
  315:17 345:14
  346:13 348:7,16
  349:16 350:7

366:19
pursuant 325:22
  350:24 393:16
put 236:12 237:18
  259:6 267:21
  269:20 271:22
  286:24 295:25
  297:21 301:22
  344:2 349:7,24
  387:14 400:20
  404:19
puts 404:9
putting 420:16

_____
          Q
_____
qualifications
  259:13 328:5
qualified 329:18
  393:17
qualifies 317:7
qualify 304:7
quality 332:4 343:7
quarter 286:8,10
queried 342:23
  346:18 350:9
  351:6 360:22
  361:10 365:13
query 343:5 344:24
  345:2 359:2
  361:17 362:25
  363:1 365:7
querying 343:18
  349:3
question 215:8,25
  217:24 218:2
  219:6 228:4
  234:16 235:20
  261:11 262:4,7,9
  262:14,18,19,20
  262:25 264:15,25
  265:3,7 266:17
  268:4 270:15
  271:13 276:3
  277:17 278:3
  279:1 280:3,6,14
  281:6,9,18,22
  283:16 288:9

296:5,7,10 299:4
300:24 316:13,15
317:8,10,12 320:6
320:25 321:2,9,24
322:1,5,9,22 323:6
323:12,17 324:13
350:19 351:14
356:2 360:13
361:7 363:4
364:19,25 365:15
365:17 366:15
367:22 397:24
400:1 409:10
417:7
questioned 297:25
questioning 238:15
  256:4 431:16
questions 214:19
  250:15 259:17
  297:22 302:7
  305:14,19 319:3
  323:3 324:9 325:1
  350:18 390:8
  392:9 402:8
  407:22 409:18
quickly 386:24
  387:9
quite 214:17 235:20
  373:9 425:20
quoted 277:18

_____
          R
_____
R 214:1 311:1 432:1
  432:1,1,1,19,19,19
  432:19
radiofrequencies
  305:8
radiofrequency
  305:6
random 356:20
range 352:17 422:24
ranges 384:9
rank 333:1,3
RAQUEL 214:9
rarely 413:22
  414:15
rate 425:7

rated 249:17
re-redirect 324:10
reach 341:19 383:4
reached 272:8
reaching 404:11
reaction 430:14
read 216:23 217:24
  218:1 227:14
  237:12 240:2
  247:11 254:11
  261:17 271:25
  278:5 282:7,13
  289:2 291:22
  315:15,23 316:19
  320:10 321:16,18
  404:3 416:21
readily 247:7,18
reading 217:22
  263:6 280:11,12
  320:22 321:22
  417:21
reads 237:9 250:3
  271:12 288:21
  291:12 292:12
  293:22 294:16
  298:13 300:4
ready 214:4,6
real 329:16 362:21
  372:3,13
really 256:1 258:25
  259:12 281:7
  328:19 380:4,5
  384:9 385:25
reason 251:11
  257:25 260:7,19
  272:7 299:11
  301:11 389:15
  407:18
reasonable 233:22
  295:23 296:19
  309:20,24 310:1,3
  310:5 313:8,11
  316:1,24 318:1,14
  318:18 403:10
  404:7,19,25
reasonably 247:8,19
reasoning 329:21

239:11,14,19
241:24 242:3,5
247:1 249:21
256:21,21 257:7
257:10,10 274:3
276:8 277:19
278:1 309:8
311:12,19 315:7
315:10,17 316:20
317:10,14,20,25
319:12,13,18,20
320:6,8,13,20,25
321:19,21 322:6,6
322:21 327:22
328:14 378:7
396:18,21,23,25
397:4,10,10,20,23
397:25 398:3,15
398:18 399:15,19
399:20 400:1,3,5,7
400:11 401:6
402:6,10,15,17,21
403:19,23 404:14
404:24 407:15,24
423:1,8 427:18,21
Reported 211:19
reporter 211:19
330:20
reports 215:11
221:6,9,12,16,19
221:22 327:2
358:21 362:17
378:5 423:4
represent 254:8
340:11 347:8
representation
375:16
representative
381:12
representatives
335:11
represented 375:13
represents 347:6
reprimanded
291:12
reputational 396:1
412:4 421:13

426:19
request 260:11
270:2,16,17 273:6
284:4 334:9 336:2
351:24 414:19,20
requested 345:5
359:2
require 227:10
257:19 307:22,24
325:11,13
required 257:20
269:9 286:14,24
292:16 314:7
317:21
requirement 309:13
requirements
269:23 295:10
research 219:16
235:2,11 242:19
244:12 246:10,24
304:10 403:5
412:25 418:22
422:24 423:3,6,9
423:16 424:23,25
431:2,4
researching 329:6
Reserve 332:21
Reserves 332:23,24
resided 263:3,5
resolve 384:4,8
resources 306:24
329:4 389:5
respect 300:25
318:2 327:9,10
347:20 353:23,25
354:3 358:7,24
423:25
respectfully 336:2
414:20
respects 372:22
respond 378:17
410:11
respondent 211:5
212:16 213:3
256:14 257:6
327:20 351:18
353:22

respondent's 307:13
327:19 345:19
351:22 357:9
375:17
respondents 270:18
371:18 396:19
responding 378:22
response 235:11
260:11 270:2,7,10
270:17,19 273:5
296:13 321:25
351:9 354:8 365:6
378:9,13,20 379:3
379:19,20
responsibilities
277:5 298:17
responsibility
278:25 279:3,6
responsible 251:1
251:10 277:6
restate 219:9 235:21
249:24
restrict 253:4
268:21
result 226:12,14,15
226:24 282:6
291:21 319:14
322:8 345:6
346:16 348:21
365:24 421:24
428:17 429:2,10
429:14 430:7,17
results 262:11,12
263:2,3 272:15
302:24 341:20
347:2,22,25 349:3
349:7,25 350:8
357:25 362:5,10
365:11,18 426:14
retained 372:25
return 326:1 345:4
375:4 380:8
383:18 385:2
returned 343:15,17
345:8 347:8 359:3
359:12,15 361:16
362:14

returns 384:18
Reuters 334:23
349:23 350:9
359:4,14,21
370:15
reveal 298:18
review 219:16
220:16 221:2,12
221:22 222:3
225:5,10 227:2,16
227:18,19 230:6
233:24 234:3
236:7 241:2,11
252:20 253:5
260:23 265:12
272:2 280:22
282:20 283:13
341:25 403:4
418:22,24
reviewed 220:17
221:6,9,16,19
226:20 239:6
248:4,16 252:22
253:1 260:11
264:20 265:14
266:24 267:3
273:4 274:17
275:15 289:10
298:6 321:14
323:14 356:10,12
358:10,11,13,16
358:21,21 408:7
411:10
reviewing 235:23
236:15,19,21,25
248:17 253:11
254:5 261:1 271:1
275:9 338:15
372:24
reviews 248:5
revised 289:6
RFID 304:12 305:3
305:5,6
Richard 377:3,10
right 214:6,20
225:13 249:13
251:19 256:15

257:4,25 258:16
259:20 270:4
274:24 275:7
276:6 278:15
280:24 281:4,6
282:11 285:5
287:1 293:9
324:14 326:3
329:11 336:6
337:8 344:11
345:23 350:3
359:18 360:5
361:5 363:13
375:7,11 376:12
376:25 386:10
388:4 410:7
415:15 428:11
431:17
rights 337:6
RIPOSO 212:4
risk 227:7,8,9 232:6
232:21 236:3
246:9 247:10,23
247:24 248:8,11
248:14,24 249:15
249:18 284:17
286:25 287:9,9
297:3,5,13 304:17
308:22 316:25
317:12,25 318:11
318:13,13,19
319:1,14 322:7,14
351:3 369:18
379:14 380:2
400:25 401:10,17
401:23 402:2,11
403:8,12,13,13,25
403:25 404:10,21
404:23 405:5,6,7
405:15 406:13,14
406:25 407:11
409:21 410:18,22
413:23 414:14
415:19 416:17
417:13,14 418:2,3
418:7 419:6,19,24
419:25 420:4,10

420:16,17,24
421:15,17 424:18
424:23 425:2,5
430:21
risks 223:9 229:16
229:22 247:8,19
308:19 318:23,24
320:2 381:20,25
382:7 421:4 430:4
RMR 432:16
road 250:25 329:23
Robert 270:25
271:2 408:9,14,24
409:7 415:25
role 400:12,13 426:9
roles 381:9
room 325:18 430:3
rooms 293:5
Roundtable 388:13
router 228:15 229:2
row 428:5,14
rows 347:7
RUBINSTEIN
212:18
rule 231:19 236:2
246:8 257:9
325:23 350:24
355:6 369:16
376:5,7 393:17
397:2
ruled 371:6
rules 232:6 294:1
322:18
ruling 347:13
349:11 372:23
398:19
rulings 336:24
run 221:20 324:4
373:24 378:2,3
running 378:4
RX 210:19 288:11
Ryan 212:7 373:12
412:24 418:20
419:2

S

S 214:1 311:1,1,1

Sacramento 339:13
355:14,17,22
358:12,17,22
370:5 404:15,24
safety 429:10
430:11
sake 347:18
sales 264:17,25
265:4,9,23 266:22
salespeople 266:7,8
266:12,15
Santa 390:21
satisfied 290:11
satisfy 240:6 290:7,9
308:3,6 309:16
savings 384:11
394:24
saw 220:9 223:25
224:5,24 236:16
237:2 247:25
248:3,3,17 306:8
372:9,10
saying 228:16
267:23 269:11,12
269:14,17,22
272:23 277:24
278:2 316:12
322:13 344:17,18
399:25
says 244:1 245:10
254:19,24 261:10
267:16 272:17
274:7 289:6
291:20 308:11
309:8 357:23
scans 222:18 224:4
224:13,18,20
scenario 273:25
scheduling 256:3
258:2
school 258:23
333:15
science 256:11
scientific 326:21
327:6,10 328:2
scope 316:6,7
353:13 354:17

367:16 396:18
screen 236:12 237:5
253:21,25 254:8,9
261:4,7 270:23
278:18 293:20
328:14 361:23
410:10
scroll 289:5
search 234:7,10
280:25 349:25
searched 240:16
seat 329:13 370:25
second 260:20
277:21 288:21
316:4 321:22
358:24 373:18
379:22 381:11
415:18 416:5
422:18
Secretary 375:25
376:2
Secrets 298:11
section 288:19
325:22
sector 303:13
secure 304:21
339:20 356:6
securing 292:21,21
294:24 295:10
304:18
security 214:23
215:6 219:5,13,15
219:19 220:3,6
226:15 230:15,25
231:19 232:20
233:19,21 234:5
234:20 235:18,24
236:2,5 237:10,15
237:21,25 238:2,3
238:7,9,19,23,25
239:4,9,22,24
240:4,5,10,15,24
240:25 241:3,5,11
241:15,25 242:13
242:23 243:1,25
244:2,7,15 245:12
245:23 246:6,8

247:8,19 250:18
250:24 279:24
285:18 290:2,2,4,8
290:10,12,15,17
290:18,22,25
291:7,16,17 292:4
292:8,12,13,22,25
293:1,2,4,7,12,16
294:6,10,12 295:3
295:7,23 296:8,15
296:19 297:1
298:25 299:24,25
300:12,19 301:22
303:24 304:4
308:3,5,6 309:1
313:16 316:2,25
318:1,14,18
319:15 322:8
326:23,25 327:4,9
327:12 328:7,21
334:7 340:3,4,11
340:15,16,19
341:17,23 342:1,8
342:10,12 343:1,2
343:6,21,22 344:1
345:8,10 346:19
346:21,25 347:9
348:17 350:10
351:7 356:14,22
357:22 358:2,3,7
359:11 360:8,15
360:16 361:19
363:3,8,11,16,25
364:3,12,13,17
365:2,23 367:4
370:3,6 371:19,22
371:23 372:6
390:21 394:18
396:4,15 398:13
398:16 400:20
403:10 404:7,19
405:1,22 411:13
412:19,25 413:7
413:13 419:16
see 215:12 229:19
237:1,5 243:11,16
243:17,18 248:8

250:7 253:25
254:3,12,14 259:7
261:7 262:14
274:10,15 276:11
288:13,19 289:7
292:10 293:21
307:9 336:17
381:22,23 383:25
388:17 397:13
403:19 413:9
423:22 424:8
427:12,15 431:13
seeing 236:17 237:3
237:4 241:12
398:18
seeking 317:10
365:25 366:12
seen 215:11 218:22
338:14 383:18
sees 424:18
sell 413:2
send 227:15,21
sense 251:3 367:21
sensitive 318:25
337:12 378:16
381:17 394:9
401:5,8 402:1
403:2,10 404:7
405:20,23,24
407:6 408:3
410:24 411:21
412:11 417:25
419:9 420:3
424:21 427:16
sensitivity 411:20
sent 343:3 345:3
sentence 216:22
277:20 291:19
315:12,15 398:9
404:3
separate 271:21,22
separated 333:1,3
340:14
separation 271:23
271:23
sequence 340:13
sergeant 333:3

series 224:21 327:1
  327:1
serious 298:17
  428:22 430:3,11
serve 332:20,22
  381:13 382:1
served 332:17,21,24
  375:13
server 223:1,7
  279:18,19 293:5
servers 222:17
  223:1,14,24 224:2
  271:15,22 274:8
  274:22 275:2,3,10
  281:25 318:25
service 223:19
  252:25 333:2
  422:15
services 260:22
  298:16 302:9
  303:23 328:23
  378:9,10,21 379:7
  379:11,24 381:24
  382:6 388:13,18
  395:17 422:16,20
  430:22
session 334:8 336:3
  336:9,15 337:19
  337:21 338:2
  352:8 373:23
  374:2 414:21,24
  415:12
set 236:1 244:23
  255:25 256:1
  295:6 308:8 329:4
  359:11 395:1
sets 240:5
setting 350:5 386:10
  404:16 414:3
  419:20
seven 240:11 242:11
  242:20,22,25
  243:24 244:2,8,11
  244:14,16 293:11
  293:14 295:4
  306:16,19 307:1,3
  307:22,25 309:9

309:11,14 327:5
severely 370:18
share 299:18 300:6
shared 279:6 299:23
  367:9 368:1
  390:22
sharing 279:25
  280:4,9 281:2,3
  299:21,21
SHEER 212:5
  256:10 257:16
  258:8,10,12
  259:19 275:19
sheet 358:1 363:6
  371:22
sheets 220:24,24
  221:2 338:22
  355:9,13,17,20
  356:1,4,5,10,12,16
  356:18,20,23
  358:10,13 359:9
  359:19 360:5
  367:7 368:1,5,10
  368:14,20 370:4
shelf 412:22 413:13
  413:15,21 414:15
Sherman 212:17
  214:5,14 215:10
  215:20 216:5,8,13
  216:18 218:8
  219:10 229:12
  232:3 238:14
  241:17,20,22
  252:11,14 253:23
  254:2,4 255:8,12
  255:20 256:17,19
  257:3,12,22 258:9
  258:11,16 259:18
  259:22 261:22,23
  270:8,11,12,21,22
  275:22 276:5,7
  278:7 284:8
  287:23 300:21,25
  301:5,7 302:2,6
  305:13 311:14
  317:3,5 319:8,11
  319:20,25 321:11

322:11,23,24
  325:3,4,9,12,15,19
  326:3,5,11,13
  328:17 330:11
  336:22 337:2,17
  345:24 346:7
  376:13 399:24
Shield 389:3
Shields 256:9,11,20
  257:14
Shohl 212:19
short 295:6 303:11
  387:8
shortly 409:21
show 312:10 369:25
  371:18 392:2,4
  427:23
showed 376:24
showing 253:21
shown 328:14
  401:20 413:1,9
  424:22
shows 220:17 363:7
  370:2 427:24
side 262:22 263:22
sign 336:11,14
significant 383:10
  403:12 404:10
  410:21 414:9
similar 407:10,11
Simmons 253:7
  277:2,4,9 278:12
  278:15,19,24,24
  279:3,8,21 280:16
simple 305:9 407:12
simpler 407:12
simply 307:13
  326:22
single 282:5
sir 215:10 216:3
  217:17,25 218:5
  228:5,19 229:3,8
  229:10,15 231:5
  231:15 255:12
  259:18 283:21
  285:10 305:24
  306:21 310:1

321:2,9 326:1,11
  332:20 333:5
  372:19 409:12
  410:4 412:7
site 371:12 372:2
sites 261:13
situation 384:2,13
situations 337:6
six 232:6 236:2
  243:3 246:9 307:4
  331:21
skip 291:10
slight 376:19
slightly 288:14
  293:19
slowdown 225:7,8
  225:11,12
small 245:22 296:2
  305:7 390:7
smaller 425:16
snuff 372:15
so-called 329:16
Social 340:3,4,11,15
  340:16,19 341:17
  341:23 342:1,8,10
  342:12 343:1,2,6
  343:21,22 344:1
  345:8,10 346:19
  346:21,25 347:9
  348:17 350:10
  351:7 356:14,22
  357:22 358:2,3,7
  359:11 360:8,15
  360:16 361:19
  363:3,8,11,16,25
  364:3,12,13,17
  365:2,23 367:4
  370:3,6 371:19,22
  371:23 372:6
  394:18 396:4
  405:22 411:13
  412:19,25 413:7
  413:13 419:16
Society 387:6
software 220:10,12
  220:13,14,14
  221:20 226:4

247:25 248:2,8,12
  263:2,5,15 283:19
  284:2,10,13,15,20
  285:12,21,23
  286:1 288:7
  295:16 297:8,8
  298:16 299:17
solely 418:16,17
somebody 286:7
  365:25 370:15
  383:15 385:25
  394:15
someone's 395:16
somewhat 256:23
sorry 217:13,17
  219:4 226:13
  238:12 252:12
  254:12,19 262:3
  262:18 264:23,24
  275:3 280:6,12,14
  281:8 282:22
  293:24 309:21
  323:6,21,24
  325:24 326:4
  343:16 356:2
  357:8 366:11
  371:12 392:14
  393:3 397:12
  399:21 410:9
  423:12 429:21
sounds 360:3
source 276:3 365:9
  372:1,3 398:23
sources 235:16
  335:22 362:7,12
  362:13,22,24
  364:6,8,23 370:13
spam 287:2,6
speak 365:20 391:4
  391:18
special 245:7,20
specialists 382:19
specialized 302:16
  326:21 328:3,6
specializes 378:12
  382:11
specialty 380:4

specific 215:1,19
229:19 232:19
233:10 235:1
244:20 245:2
247:23 265:17,18
265:20,21 266:4,9
269:3,5 270:3
273:19 275:6
282:15 290:10
300:8 307:19
314:5 403:5,20
404:12 406:22
423:24 428:2
specifically 220:5
235:12 240:20,22
246:1,15 247:21
254:18 260:12
264:2 279:20
280:23 302:18
304:1 305:3 307:4
334:11,15 380:22
381:22 384:1,20
391:2 393:24
394:17 404:13
405:20 410:5
411:10,14 412:19
412:24 413:4
416:2 422:7,25
423:20,21 424:12
424:25 431:3,5
specification 268:16
279:13
specified 230:3,4,7
268:19 302:16
specify 260:15,17
264:7 269:6,23
270:2 272:9,12
295:13 297:8,14
313:23 314:3,13
specifying 245:15
speculate 366:3
speculation 366:2
speed 372:14
spelled 377:10
spelling 432:22
sponsor 426:13
sponsors 426:11

spouse 385:11
spreadsheet 343:3,4
343:14 344:24
345:7,8 349:8
359:20,24 360:21
361:11,14,16
366:8 371:5
squared 331:2
staff 223:19 225:10
263:19 272:12
333:3 402:9
stand 342:18 369:6
370:10 373:24
376:17
standard 309:3,6
328:1
standards 230:13,15
230:19,22,24
231:1 232:10,13
233:14 234:7,14
234:18,20,24
235:5,19,23 236:5
242:19 246:2
294:1 307:14,16
390:20 391:3
394:4
stands 232:15
288:23
start 236:19 258:3
281:17 311:11
316:11 387:22
431:15
started 236:21
258:5 361:24
380:5
starting 271:11
405:5 422:25
starts 405:18
state 226:17 275:12
275:14 280:22
319:13 322:6
332:4 334:4
361:20 379:5
stated 221:19
230:10 237:23,24
237:24 242:24
244:19 245:13

263:14 265:17,25
266:10 272:13
275:9 284:25
290:16 292:1
294:8,13 299:9
300:15 301:11
314:22 320:24
321:5,9 329:14
371:3 382:10
401:6 409:7
415:25 417:22,22
statement 215:16,19
215:21 225:2
230:15,17 231:10
233:9 236:23
264:3 267:20
268:15 269:3
294:9 371:9
statements 229:19
265:15,21 266:4
states 211:1 268:7
272:22 273:6
332:18,21 400:20
stating 244:22 266:6
268:3,20 323:7
371:13
Statistics 423:5
status 336:5 379:1
380:8 383:19
385:3,17 414:23
415:2
stay 337:7
stemmed 388:11
step 327:16
steps 282:24 405:4
stipulation 375:14
stolen 368:10
storage 231:8
store 305:11
stored 318:11
strategy 306:4,15
308:1 309:6 423:5
street 361:20 413:6
stricken 321:13
389:12
STRICKEN/REJ...
210:15

strike 273:9 330:5
389:25 395:21
421:15
strong 245:15
295:17
stronger 282:1
structured 377:24
377:25
students 304:15
studies 333:10
401:19
study 304:20 423:16
423:18,21,23
424:1,9,12 425:13
425:17,18 426:10
426:12,14
stuff 215:12
subject 278:4
294:20 298:21
336:8,19 337:2,9
337:13 349:14
subjective 407:13
submit 261:4 270:24
278:18 280:8
369:18
submitted 327:22
359:10,20,25
375:19 400:8
subparagraph
237:7 247:15
250:3 252:15
259:24 274:6
277:18
subparagraphs
249:24 311:15
subset 425:16
substance 327:25
substantial 403:24
403:25 404:9
substantiated
370:14
substantive 403:13
suffer 394:10,21
421:9 422:9 426:6
426:18,23
suffering 427:25
sufficient 248:23

252:4 290:7,21
291:14,24 293:7
299:10 312:10
323:18 324:1
350:23 369:16
sufficiently 290:23
296:21 371:15
suggest 257:4
261:19 352:2
suggested 296:24
suggesting 241:4
301:6
Suite 212:21 213:9
summarize 390:1
superseded 375:20
supervision 384:8
suppliers 298:15
support 230:9
233:11,16 234:8
235:25 239:7
240:16 275:13
330:8
supported 230:19
275:2
supports 273:5
suppose 285:12
supposed 252:5
280:1
sure 225:2 235:22
258:17 262:12
267:19 269:8
270:14 275:21
279:5,7,10 282:15
282:18 285:6
287:25 325:17
326:2 338:7 346:9
353:7 360:12
380:21 381:23
407:9
Survey 431:6
survive 256:1
susceptible 226:5,7
226:13
suspect 416:7
suspected 416:8
sustain 344:12
366:20

sustained 322:10
  355:6 367:19
  392:22
switch 239:12
sworn 214:11 331:3
  331:8 371:7,8
  377:5
synonymously
  402:19
system 244:23,25
  248:24 279:16
  294:10 295:11,24
  343:5 349:24
  360:22 365:14
systems 292:13
  387:6 414:11

T

T 311:1 432:1,1,1,19
  432:19
tab 397:14
take 227:13 231:25
  245:1 255:2,3,14
  267:21 270:17
  303:14 305:18
  310:8 336:14
  368:5 376:18
  383:8 387:9
  394:24 397:9
  401:16 418:2
  419:18,24 420:15
taken 255:7 272:14
  306:3 310:17
  327:2,6 432:9
takes 383:24
talk 221:12 226:19
  256:3 258:13
  305:21 347:22
  400:11
talked 256:5 295:2,4
  306:17 385:25
talking 217:19
  218:24 234:18
  276:2 280:8 282:9
  282:10 283:17
  309:8 312:22
  320:22 323:10

412:11
talks 232:21 299:20
  308:7
task 269:10 367:13
  367:14
tasks 314:5,7
tax 384:14
taxes 384:17
team 235:11 378:3,5
  378:7 380:16
  381:11,18 382:3
  383:16 386:4
teams 384:7
technical 277:12
  326:21 328:3
techniques 334:21
technology 234:21
  304:12,13,19
  305:3,5,6
tell 280:10 312:20
  348:1 349:15
  363:18 364:14,16
  389:8 415:10
  420:20
telling 259:5,15,16
ten 306:12 429:15
tender 351:22 394:2
tendered 366:13
tendering 351:19
  393:17
tens 386:4
tenure 261:13 278:9
  278:13
term 238:1 240:23
  306:1 360:24
  404:23
termination 291:21
  294:21 298:22
terminology 239:2
terms 241:25 243:17
  243:18 245:10,13
  248:11,14 262:20
  292:20,21 294:24
  301:16 302:8
  303:9 323:13
  328:20 337:5
  347:16 367:14

402:15,18 425:2
  425:22
test 248:9,25 249:6
  267:13 273:12
  302:24 407:19
tested 393:24
testified 214:11,17
  221:15 230:12
  234:13,17 276:17
  311:22 312:9
  313:4,9,22 315:11
  316:12,17 322:25
  324:18 328:19
  329:2 331:8 353:8
  354:1 367:14
  377:5 378:12
  389:18 390:24
  402:6 405:14
  408:24 411:6
  413:12 415:20
  416:16 417:12
  426:17
testifies 317:13
testify 256:25
  317:18 347:24
  370:8,22 409:23
testifying 280:16
  347:14 349:7
testimony 214:20
  221:5,14 224:1,8
  224:10 229:21,25
  230:16 234:24
  235:23 238:18
  248:16 253:5,12
  253:19 254:5,10
  254:11 260:6,23
  261:1,6 263:8,12
  263:13,18,18
  264:20 265:12,14
  266:11,11,24
  267:2,8,15 268:22
  269:5 270:25
  271:1 272:2,12,16
  272:21 273:3,3,4
  274:13,17 275:24
  275:24 276:1,23
  277:4,8 278:16

280:20,22 281:16
  282:12 283:9
  284:9,12 311:23
  311:25 312:11
  313:6,25 314:22
  315:13 316:5
  321:12 322:13
  324:20 325:21,22
  326:10,19 328:2,9
  330:6 339:5
  344:16 347:19
  349:9 353:7 355:8
  358:20 367:12
  369:22 389:11,11
  389:16,22 402:17
  408:9,14 409:7
  410:1 415:24
  416:4,18 417:4,22
  418:6,13,17
testing 272:21 276:9
  276:17,22 277:11
  297:10 302:14
tests 263:24 302:15
text 409:2
thank 215:18 216:4
  218:6 229:11
  254:17 255:12,20
  259:20 270:20,21
  284:7 287:22
  305:13 310:7
  311:5 317:22
  319:5 320:16,17
  322:11,23 324:25
  325:5,6 326:7
  328:16 329:11,12
  330:9,11,12,14,24
  330:25 333:6
  337:16,17 338:8
  342:21 344:20
  345:17 346:4,11
  348:3 352:4,9,11
  353:16 354:19
  357:18,19 366:22
  367:23 369:5
  370:24 371:1
  372:19,21 373:3,6
  373:10 374:1

376:11,12,15
  390:12 397:6,13
  400:9 410:7
  415:16 417:9
  431:18
theft 217:3,4 315:19
  315:20 334:1,3,7
  352:24 370:9
  371:21 378:11,11
  378:25,25 380:23
  380:24 382:11,12
  382:14,23 383:1,7
  383:10,11,15,15
  383:21,22,23,25
  384:6,7,9,13,19
  385:2,4,5,10,11,19
  385:20,24 386:8,9
  386:12,13,17,17
  387:18 388:19,23
  389:20,21 390:16
  390:17 391:5,5,19
  391:19,23,23
  393:18,19 394:12
  394:13,14,15,19
  394:21 395:8,14
  395:15,21,24,25
  396:3,10,12 399:2
  399:5 400:15,15
  400:25 401:1,11
  401:12,17,18
  402:12 403:1,2,6,6
  405:6,7 409:9
  410:22,23 411:22
  411:23 412:5
  413:25 416:9
  417:14,14 418:7,7
  418:23,23 419:6,7
  420:5,6,11,12,17
  420:18 421:3,9,17
  421:24 422:3,25
  423:16 424:5,6,8
  424:14,23,24
  425:1,3,8,11,12,14
  426:3,7 427:15,25
  428:7 431:4,6
theory 369:12,14
thief 368:11 382:20

384:15 394:23 395:1 406:10 411:25,25 422:17 422:17 429:25 430:1
thieves 366:7,17 367:16 368:11 380:8 382:16 410:14,15 413:1 413:25
thing 216:14,14 217:16 218:4 244:22 252:25 255:23,24 258:18 269:22 277:25 282:5 328:17 402:18
things 223:4 225:14 225:22 244:23 249:12,14 250:9 255:6 286:23 295:22 394:17 402:22 422:14
think 214:4 224:19 224:21,23 230:17 232:15 234:9 236:14,23,24 237:2,19 240:18 241:6,7,9,10 246:7 246:14 255:22 258:12,13 259:4,6 260:15 267:8,11 267:15 277:4 279:13,14,18 281:5,12,24,25 282:3,4,6 283:18 286:20,21 287:24 288:9 293:10 294:4,15 295:25 297:2 298:5 301:2 301:5,20 302:1 306:13,18 309:7 310:9 313:20 314:12 317:8 319:20 320:1,9 326:3,17 328:5,9 329:7 330:7,7

336:22 337:7 349:11 354:4 359:1 363:22 364:5 366:10,11 366:16 367:12,16 375:22 376:21,22 385:8 393:1,4 416:23 417:6 420:23 424:20 425:25 428:8 429:19
thinking 236:22
third 250:2 380:4 406:11 415:18 416:5 422:20
third-party 223:19
Thomson 334:23 349:23 350:9 359:4,14,21 370:15 371:9 372:1
thought 217:17 256:6 338:4 343:25 373:16
thousand 222:16 252:24 381:4
thousands 386:5 420:22
threats 251:11,12 430:11
three 277:13 283:6 340:13 372:10 379:13 406:4,5 421:12 422:14
threshold 327:20
throw 399:18
Thursday 258:3,4
tie 356:22
ties 353:7 357:23
time 214:17 221:25 224:3,12,16,18 228:7 237:1 243:7 243:9 246:13,17 253:16 276:22 277:1,9,13 279:17 283:3,5 287:12,14 301:8 302:10

303:4,12 310:9 311:20 321:3 323:1,8,13 324:5 324:19,22 336:1,6 344:14 345:14 346:14,24 347:13 348:2 349:7 350:21 351:20 352:3 355:5 365:21 373:7 376:1 377:23 397:2 412:22 415:7,8 416:25 428:8 431:14
timely 318:9 429:9 430:22
times 248:1 288:23 380:14,20 408:18 408:20 412:18
timing 419:14
tired 301:1
title 377:13 432:4
titled 338:22
Tiversa 408:11,12
today 316:8 328:9 355:8 389:1 393:6 402:17 414:9,11 425:10 431:15
told 339:12 416:22
tomorrow 431:19
tool 335:2
tools 421:3
top 300:3
topic 386:21 391:17
total 431:12
totally 371:15
touché 398:19
touched 411:2
track 399:19 400:1
tracks 241:24
Trade 210:1 211:1 211:14 212:3,8 298:11 331:16,20 331:25 332:1 333:19,22 334:20 335:3 338:25 339:4 402:24

411:3 431:1 432:10
traditional 377:25
traffic 227:25
training 251:2 258:23 299:13 334:21 335:6,10 335:10,12,14 340:12
trainings 335:9
transaction 338:23 421:6
transcript 274:13 276:14 278:19 416:19 432:7,8,21
transcripts 263:13 275:9
transfer 231:8 285:1 388:17
transferred 312:24
transfused 430:3
TransUnion 362:17
treated 353:22
treatment 300:8 427:2 429:2,7
trend 243:11,21 307:7
trial 210:4 211:9 215:13 371:6 400:8
trier 328:4,8
trouble 399:22
true 225:5 228:20 264:25 265:3,23 266:1 276:16,19 311:19 386:5
trust 385:9 415:11
truth 370:22
try 296:10 303:10 321:18 325:19 366:24 395:4
trying 221:20 233:18 268:11 269:16,23 277:25 296:16 304:21 309:10 357:17 372:13 373:20

407:3 425:4
tune 414:9
turn 216:13 227:14 239:17 247:1 249:21 262:2 274:3 279:21 281:15 292:7 297:24 300:2 319:12 322:5 334:18 336:11 398:2 402:6 411:4 415:18 427:6 428:4
turned 229:2 336:14
turning 417:11 427:23 428:14
turnover 251:6 301:17
twice 380:14 391:21
two 239:12 246:21 246:23 257:5 267:9 268:13 276:25 283:6 291:11 330:18 336:4 340:13 357:15 381:9 404:13,16 405:4 416:17 418:21 419:1
type 215:1 217:6,7,9 282:1,3 292:22 302:8 318:23 372:6 394:20 411:7 430:1
types 217:2 223:9 235:8,14 253:2 260:16,17 268:17 269:6,9 273:18 297:9,16 302:15 313:23 314:3 315:18 324:7 379:2 384:6 391:7 394:9 396:2 400:23 421:8
typically 378:15,21 379:22 380:12 381:9,15 382:2,5,8

383:5,9 394:21
395:12 413:15,20
419:17

U

U.S 334:4 388:14
391:16 424:14,15
425:14
Uh-huh 398:10
Ultimately 370:21
unable 221:20 253:1
253:25
unauthorized
220:13,19 226:4
248:6 284:1,10,12
285:8 299:17
312:3,5,5,7 317:12
318:2 378:16
379:10 380:10
381:1 394:8 396:8
401:4,8 402:14
403:14 407:5
410:23 417:15
418:8 420:2
421:10 424:17
427:15
understand 218:20
231:12 235:20
251:13 252:4
255:8 285:7
286:18 290:13,24
299:24 304:12
309:2 323:24
337:5 349:11
350:25 354:12
355:8 360:12,21
362:11 373:5
380:1 381:20
383:13 385:4,20
400:9 407:12
409:25 418:2
419:23 420:10,24
420:25 425:15
understanding
256:19 263:20
264:1 265:7,22
266:8,14,17

269:20 271:9,14
278:10,23 279:2
284:19 285:16
299:16 304:16
306:3 324:6 328:4
335:15,19,20
338:24 339:2,3,6
344:9 347:21
355:12 358:5
362:4,9,12 376:13
388:2
understands 383:6
understood 258:8
346:4 357:9
358:20 371:18
392:25
unfair 322:17 351:3
369:19
unfortunately
383:23 385:10
386:7 401:13
412:25 420:7,13
unintentional
313:18
Union 338:21
unique 385:22
United 211:1 332:18
332:21
UnitedHealthcare
389:2
universe 424:7,19
431:12
universities 379:8
University 256:12
333:10,14
unlimited 262:7
unrealistic 257:18
unreasonable
307:13 313:21
unused 245:15
unusual 223:10
updates 245:14
295:16
upwards 413:11
usage 277:11 288:22
291:6
use 223:14 234:11

237:14 245:19
250:4,11 252:16
259:24 260:8
277:11 288:6
289:18 297:15,17
298:19 304:11,13
304:18 306:8
330:19 335:6
346:10 360:8
367:10 368:2
371:17 372:13
395:4,10 402:15
402:19 405:4
407:7 413:1 414:1
414:6,7 423:8
425:7,9,22
uses 289:19 362:22
364:5 394:15
395:16
usually 225:7
utilities 362:23
utility 335:22 362:8
372:4
utmost 309:20,25

V

vague 238:5
valuable 411:24
value 351:12,13
354:5 370:18,19
413:6
Van 256:7 258:9
VANDRUFF 212:4
325:24 326:4,7
330:14,25 331:9
331:13 333:6,7
336:1 337:10
338:3,8,11 339:8,9
342:21,22 344:15
344:20,21 345:15
346:4,15 347:17
348:3,4,23 349:1
349:11,21 350:1,4
350:17,21 351:18
351:21 352:4,9
353:6,16,23
354:16,19 355:2

357:2,5,8,17
366:10,16,22
367:11,23 368:21
369:11,14 370:2
371:1 372:18,21
373:3,5,10 375:9
375:12,24 376:10
varied 372:3
variety 244:13
297:11 333:22
335:21 362:7,22
362:24 364:6
various 223:4 266:4
273:7,7 274:2
297:5 306:18
309:15 394:19
401:23 406:23
428:1
vehicles 293:23
verify 336:18
versed 383:24
versus 425:4 431:12
victim 380:6,23
382:14,19 383:14
383:18,25 384:10
384:14,16,22,24
385:1,10,24 386:8
395:21,24,25
396:9 400:25
401:23 418:3
420:17 422:2,15
422:15 423:22
424:5
victim's 394:24
395:2 429:24
victims 352:24
378:10,25 382:11
382:23 383:1,21
383:22 385:11
386:5 394:21
403:1 421:24
422:9 425:10,11
426:2,2,5 427:24
428:2
video 286:11,15,16
286:21,22
view 386:1 409:3

viewed 406:12
415:22 424:3
431:11
violate 294:15
299:15
violating 290:14,25
291:15,25 294:11
violation 292:3
298:21
violations 291:9
virus 223:20,25
224:5,25 225:12
225:17,25 226:2
226:13,14,16
viruses 221:17
222:5,11,16,17,19
222:20,22,24,25
223:6,17,18,22,24
224:1 225:6,14,22
voice 264:9 301:1
VOIR 210:8
VOLUME 210:4
211:9
voluminous 233:1,2
345:19
vulnerabilities
229:22 230:2
247:9,20 249:2,6
249:16 251:15
295:20 296:14,16
296:17,22,24
297:20 307:18
308:20,22 318:7
318:20
vulnerability 248:10
248:25 297:10
vulnerable 249:12
249:14

W

Wait 217:12
wallet 368:14
want 214:18 235:7
235:22 244:22,24
253:20 256:3
258:1,2,19 259:6
260:6 274:3

275:22 285:6
287:19,24 288:17
301:2 308:23
320:4,5 322:12
325:20 347:14
366:23 367:20
371:17 376:18
381:22 399:17
416:24 418:11
wanted 246:16
258:18 357:10
360:25 361:3
375:21 388:17
407:9
wants 381:18
warning 415:5
Washington 211:16
212:12,22 213:10
wasn't 225:3 248:21
248:23 280:1
284:25 304:23
364:25 365:8
368:3,8,12
watch 286:6
watches 286:7,9
watching 286:21
water 264:11,12
wave 373:20
way 242:25 249:19
255:25 258:6
267:21 271:14
273:24 296:11,24
298:18 306:5
308:24 312:2
315:3 359:15
376:6 401:3,7
407:12 416:21
417:18 419:8
425:25
ways 267:22 274:2
386:11
we'll 257:19 258:13
278:5 310:13
325:19 330:23
373:22,25 375:4
431:17,19
we're 214:4 255:3,5

255:16,17 280:8
282:9,10 288:10
310:15 319:23
325:18 336:9,22
344:17,18,18,19
353:12 359:17
363:22 373:18
375:3,5 376:8
390:9 407:3
415:13 428:11
431:21
we've 237:19 238:10
276:17 295:2,3
379:4 381:3
382:16 384:20,23
386:16
weakest 313:15
Web 371:12 372:2
weeds 390:10
week 375:19
weeks 382:9
weigh 369:22
weight 330:1
welcomed 336:14
well-known 237:22
329:8
Wells 365:25
went 234:7 258:23
343:1,12 359:18
weren't 323:18
324:1,6 355:19
360:9
West 334:23 359:4
Western 338:21
Whalen 211:19
432:16
white 386:19
whoa 217:12,12,12
wholly 371:14
wide 362:24
willfully 367:9
WILLIAM 212:17
william.sherman...
212:24
willingly 368:1
Wilmer 210:11
330:15,16 331:6

331:14,16 332:17
334:11 335:15
336:4 338:4,5,12
339:15 340:5,23
344:22 346:16
347:20 348:5
349:1 350:2,5
351:5 352:15
353:25 354:9,24
355:9 357:21
359:14 366:12
367:13 368:18
369:19 370:16
Wilmer's 330:19
353:7 369:22
wish 347:19
withdraw 257:13
366:25 375:18
376:3 417:1,4
withdrawal 376:6,6
427:4
witness 210:8
214:10 215:16,19
216:3 217:17,21
217:25 218:5
228:5,10,19,22
229:3,8,10 238:12
254:22 256:3,6,15
256:20,21 258:4,4
258:21 259:5
261:20 270:15,19
271:20 275:20
283:21,25 285:10
285:14 286:9,16
287:6,14,18
295:10 300:22
301:4 305:24
306:1,10,13,21
307:3,15,24
308:13,16 309:5
309:14,21 310:1,5
317:18 320:21
321:1,4,8,25 325:8
325:16,22 330:13
331:2,7 333:5
342:16,18 343:20
344:13 351:15,19

351:22,25 352:3
353:18,24 354:20
354:21 367:18
368:25 369:4
370:8 371:20,25
372:17 373:8
375:8 377:4
392:11,19 393:18
396:24 397:25
400:2 409:12,13
412:7 416:12
word 312:1,2 359:10
359:22 400:5,5
403:19,23
worded 240:21
320:24 321:1
wording 320:19
words 223:11
309:20 403:25
work 225:7 257:5
259:10 271:5
292:16 298:13
304:22,23 305:2
332:8,12 333:13
333:18,20 334:10
334:12,15,18
341:13 342:3,7
347:19,23 348:5
348:14 353:9
354:1,4 365:24
382:20,25 383:16
383:20 384:3,3,23
387:10 388:5,7,11
389:7,9
work-related 294:3
worked 259:10
303:12 304:15
331:19 332:10
354:24 377:22
381:1,3,5,7 382:23
384:20 386:11
390:18
working 223:2,8
292:14,16 295:13
332:12 334:2,3
384:1,7 386:3,15
386:22 389:14,17

389:20 390:18,24
402:25 406:17,18
420:21
works 357:13
399:13
workshops 334:6
workstation 220:20
workstations 220:11
worth 413:8,10
wouldn't 243:17
285:14,19,19,22
290:24 299:5
300:13 309:5
371:7
wrangling 232:16
write 227:12,21
392:3
writing 250:19,20
250:25 251:5,16
265:19,25 268:25
283:9 299:5,8
300:17,19 301:9
301:12,22
written 240:6,7,9
246:12 289:13
290:7 300:10
wrong 221:15 278:5
427:2 430:2,7,10

X

X 210:2

Y

yeah 403:22 404:5
406:5 417:9
429:19
year 306:12 333:16
years 249:3 283:6
306:12,12,14
331:21 332:11
380:5 386:14
391:11 401:20
402:25 406:24
yes-or-no 300:23
yesterday 214:18,22
230:12 232:16
234:13 256:5

259:1 283:18
297:25 298:5
316:1,5,12,12
328:10 375:12
376:1

Z

zip 361:21

0

0010 414:22
0085 415:1
04 427:7,17,20,23
430:23 431:9
0742 397:10,12,15
0930 431:20

1

1:03 310:16
10 236:11 237:7
241:24 249:24
100 365:12,19
100(d) 320:10
321:15
106 261:6
108 254:25 261:10
109 262:2
11 281:17 402:25
428:19 429:4
11:20 255:16
112 264:13 266:16
113 266:19
120 414:10
13 264:24 279:21
280:12 388:9
138 271:11
139 253:8
14 280:15
15 281:21 310:12
15,000 391:16
155 281:15
16 249:21,23 252:15
259:24 262:3
325:22 332:11
17 398:2 399:15
400:11
1718 218:14,17,21

218:22,25 219:2
219:11,17,22
220:18 312:11
407:23,25 408:8
409:1,6 410:20
411:9,10 412:12
413:15 414:22
416:2 417:16
418:15 420:4
421:11,18,25
426:20,22 428:16
429:1,13 430:6,16
18 216:19,22 254:19
262:2 327:23
19 239:11,17 264:23
1919 213:8
1993 300:5
1999 303:17,18

2

2 210:4 211:9
297:24 298:5
375:14,18,20
376:8
2:10 310:14
2:12 311:2
20004 212:22
20006 213:10
2003 377:21
2004 289:6,17
2005 222:1 323:1
324:19
2006 423:2
2007 341:10
2008 283:1 305:2
331:22 408:10,13
408:18,21
2009 305:2 341:11
2010 222:1 224:21
224:23 248:9
276:18,22 311:21
323:1 324:19,22
324:24 393:15
2011 408:22,23
2012 388:11 389:13
2013 236:22 361:25
362:2 387:14,23

388:21 389:14
408:25 423:15
431:3,6
2014 210:6 211:7
432:5,13
202 212:13,23
213:11
20580 212:12
21 210:6 211:7
432:5
214 210:9
22 271:12 357:1,12
24 247:1
25 432:13
27 320:10 321:15
422:6,9 425:24
426:5
2L 333:16

3

3 340:8,22 341:3
3.31(a) 393:17
3.41(b) 325:22
3.43(b) 325:23
350:24 369:16
30 430:18
31 240:12
311 210:9
319 210:9
324 210:10
326-2999 212:13
331 210:11
34 274:12
35 311:13 388:21
352 210:11
36 274:3 276:8
372-9100 212:23
377 210:12
38 315:7

4

4:00 375:4
4:30 258:4
40 388:21,21
41 400:20
44 338:22 340:1,6
45 249:23 252:16

451 345:12 348:7,10
348:15 350:7,13
350:22 351:3
353:11 354:3
369:11,20 371:3
372:16,25
49 216:23 315:9,16
316:20
499-2426 213:11

5

5 264:14 279:23
298:2,3,10 338:22
339:25 340:6
408:10,21
5:33 431:23
52 239:19 309:7
53 377:19
58 253:7

6

6 264:23 300:2
600 211:15 212:11
340:18
610 212:21
63 247:5
650 213:9

7

7 408:22
7:00 257:21,21
700 340:19
702 325:23
71 288:11
719 270:24
724 261:5
730 278:17
740 216:7,7,9
311:13
750,000 404:20
405:1
76 320:9 321:16
422:1 425:10,24
426:1

8

80 414:10

800-30 232:18
801 212:20
81 253:18 254:9
82 332:25
85 338:5,13,19,20
339:10,14,19,21
339:24 340:6,17
340:18,21,22,24
341:2,5,8,10,13,23
341:24 342:8
343:2,8 344:24
346:19 347:10
348:17 350:10,14
351:8,24 356:8,12
357:1,4,12 358:16
359:23 363:21
365:3 369:2 370:3

9

9 292:7 403:23
404:3 408:23
9:37 211:8
90 255:24
91 277:19 311:12,15
311:19
92 311:16
9300 408:4 417:24
422:2
9357 211:4 214:3
432:3
94 332:25