

EXHIBIT

8

In the Matter of:

LabMD, Inc.

September 25, 2013
Initial Pretrial Conference

Condensed Transcript with Word Index



For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

1

1 I N D E X

2

3

4 CASE OVERVIEW: PAGE:

5 BY MR. SHEER 8

6 BY MR. RUBINSTEIN 22

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

3

1 APPEARANCES:

2

3 ON BEHALF OF THE FEDERAL TRADE COMMISSION:

4 ALAIN SHEER, ESQ.

5 LAURA RIPOSO VANDRUFF, ESQ.

6 MEGAN COX, ESQ.

7 MARGARET LASSACK, ESQ.

8 RYAN MEHM, ESQ.

9 Federal Trade Commission

10 Division of Privacy and Identity Protection

11 601 New Jersey Avenue, N.W.

12 Washington, D.C. 20001

13 (202) 326-2999

14 asheer@ftc.gov

15

16 ON BEHALF OF RESPONDENT:

17 REED D. RUBINSTEIN, ESQ.

18 Dinsmore & Shohl LLP

19 801 Pennsylvania Avenue, N.W., Suite 610

20 Washington, D.C. 20004

21 (202) 372-9100

22 reed.rubinstein@dinsmore.com

23

24 ALSO PRESENT:

25 Victoria Arthaud and Hillary Sloane Gebler

2

1 UNITED STATES OF AMERICA

2 FEDERAL TRADE COMMISSION

3

4

5 In the Matter of:)

6 LABMD, INC.,) Docket No. 9357

7 a corporation.)

8 -----)

9

10

11

12 INITIAL PRETRIAL CONFERENCE

13 SEPTEMBER 25, 2013

14 2:00 P.M.

15 PUBLIC SESSION

16

17

18

19 BEFORE THE HONORABLE D. MICHAEL CHAPPELL

20 Administrative Law Judge

21

22

23

24

25 Reported by: Susanne Bergling, RMR-CRR-CLR

4

1 P R O C E E D I N G S

2 - - - - -

3 JUDGE CHAPPELL: Okay. Call to order Docket

4 9357, In Re: LabMD. Is there a space after the B or is

5 that one word, "LabMD"?

6 MR. RUBINSTEIN: It is one word, Your Honor.

7 JUDGE CHAPPELL: Okay. Thank you.

8 I will start with appearances of the parties,

9 and I will start with the Government. Go ahead.

10 MR. SHEER: Good afternoon, Your Honor. I'm

11 Alain Sheer representing the Commission.

12 MS. VANDRUFF: Good afternoon, Your Honor.

13 Laura VanDruff, Complaint Counsel.

14 JUDGE CHAPPELL: Okay.

15 And for Respondent?

16 MR. RUBINSTEIN: Your Honor, Reed Rubinstein

17 representing Respondent. If I could, I would like to

18 take this opportunity to thank you and to thank

19 government counsel for their accommodation of my

20 schedule. It is very much appreciated.

21 JUDGE CHAPPELL: You're welcome. I would expect

22 that request to come a little sooner next time.

23 MR. RUBINSTEIN: Yes, Your Honor.

24 JUDGE CHAPPELL: And also, just so everyone

25 knows, we do follow motions practice, and I will need a

5

1 motion from here out to deal with something.
 2 MR. RUBINSTEIN: Thank you.
 3 JUDGE CHAPPELL: I notice that we have got more
 4 than two people listed at on least one side. Our office
 5 will email courtesy copies of orders to the parties.
 6 That's courtesy copies. Official service is made by the
 7 Office of the Secretary. I will need each party to
 8 designate no more than two individuals to receive
 9 communications from my office. You can send an email to
 10 my assistant, Dana Gross, or just to the OALJ Web site,
 11 and give us the two people you want to receive courtesy
 12 copies from my office.
 13 I think for the first time in history we have no
 14 modifications to the draft scheduling order. So, thanks
 15 to both of you. I will issue that order by tomorrow or
 16 Friday. I think I'm obligated to get it out by Friday
 17 under the latest rules.
 18 There's a limit to the amount of time we're in
 19 trial. I don't anticipate us getting anywhere near the
 20 limit. Does -- while we're here, how many witnesses do
 21 you anticipate for the Government? I just need a
 22 ballpark. I'm not holding you to anything.
 23 MR. SHEER: Judge, I'm watching the monitor. We
 24 expect that we will be putting on seven or eight
 25 witnesses.

6

1 JUDGE CHAPPELL: Okay.
 2 And for the Respondent?
 3 MR. RUBINSTEIN: Approximately the same number.
 4 JUDGE CHAPPELL: I'm thinking this is going to
 5 move along fairly quickly. Any experts?
 6 MR. SHEER: Yes, Your Honor. We are going to be
 7 using experts on technical issues and also on consumer
 8 injury.
 9 JUDGE CHAPPELL: You need to stand up when you
 10 speak. She needs to hear you. Use that microphone.
 11 MR. SHEER: Sorry. We are expecting to use
 12 technical experts and also experts for consumer injury.
 13 JUDGE CHAPPELL: Okay.
 14 MR. RUBINSTEIN: Your Honor, we also will be
 15 using --
 16 JUDGE CHAPPELL: If you -- if you use that
 17 microphone -- just stand and use one of the microphones,
 18 either one. You have got one over in the middle.
 19 MR. RUBINSTEIN: This one works, if it works for
 20 you.
 21 We will also be presenting expert testimony,
 22 rebuttal testimony to the Government's witnesses. We
 23 anticipate there will be two, perhaps three, that will
 24 go to harm and will also go to the technical issues
 25 associated with the file theft.

7

1 JUDGE CHAPPELL: Okay. Under the current rules,
 2 the hearing is limited to no more than 210 hours. So, I
 3 need the parties to develop a system or mechanism to
 4 keep track of that, although I don't see us stretching
 5 those boundaries in this hearing.
 6 Regarding -- one thing regarding the scheduling
 7 order, let me talk about dispositive motions. I didn't
 8 put a deadline on the scheduling order for summary
 9 judgment motions. There is a rule that covers that, if
 10 you intend to file a summary judgment, and if you don't
 11 know, I'll tell you.
 12 Summary judgments will be ruled on by the
 13 Commission, the same body that voted to issue the
 14 complaint in this case. With respect to motion to
 15 dismiss or other substantive motion, the rules provide
 16 that if they are filed before the start of the
 17 evidentiary hearing, they will be ruled on by that same
 18 Commission; however, motions to dismiss or substantive
 19 motions filed after the start of the evidentiary hearing
 20 will be decided by me, not the Commission.
 21 Have there been any settlement discussions?
 22 MR. SHEER: There were very, very preliminary
 23 settlement discussions; that is to say that Respondent
 24 LabMD had indicated they had interest in settlement at
 25 one point long ago, but the parties did not pursue it,

8

1 and at this moment, there are no settlement discussions
 2 on the table or ongoing.
 3 JUDGE CHAPPELL: Any comment on that?
 4 MR. RUBINSTEIN: That is correct, Your Honor.
 5 JUDGE CHAPPELL: At this time, I allow each side
 6 to present an overview of their case, and I limit it to
 7 15 minutes, and I'll let the Government go first;
 8 however, I'll let you know, if I ask questions, I will
 9 add to your time, or take up any of your 15 minutes.
 10 Go ahead.
 11 MR. SHEER: Thank you, Your Honor. LabMD is a
 12 medical laboratory that tests blood and tissue samples
 13 that doctors take from consumers. In doing so, it's
 14 collected very sensitive information about hundreds of
 15 thousands of consumers, including names, Social Security
 16 numbers, checking account information, and medical test
 17 results.
 18 JUDGE CHAPPELL: Hundreds of thousands. So,
 19 you're saying they do a national business?
 20 MR. SHEER: They do a national business.
 21 LabMD exposes this treasure trove of information
 22 to people who never should have had access to it by
 23 failing to take reasonable and appropriate security
 24 measures. Identity thieves use consumers' personal
 25 information to impersonate them in a variety of ways,

1 depending on the information. For example, financial
2 information has been misused to open new -- to conduct
3 credit card fraud and to go into bank accounts; and
4 medical information has been misused to steal insurance
5 benefits. In each of the last ten years, identity theft
6 has been the number one complaint that the FTC has
7 received. There were 369,000 complaints in 2012.

8 The personal information that LabMD maintains is
9 information that identity thieves want. This was action
10 was brought under Section 5 of the FTC Act. Section 5
11 provides the Commission with broad authority to address
12 new areas and practices as they develop.

13 JUDGE CHAPPELL: Have you -- in that regard, has
14 the Commission issued guidelines for companies to
15 utilize to protect this information or is there
16 something out there for a company to look to?

17 MR. SHEER: There is nothing out there for a
18 company to look to. The Commission has entered into
19 almost 57 negotiations and consent agreements that set
20 out a series of vulnerabilities that firms should be
21 aware of, as well as the method by which the Commission
22 assesses reasonableness.

23 In addition, there have been public statements
24 made by the Commission, as well as educational materials
25 that have been provided. And in addition, the industry,

1 the IT industry itself, has issued a tremendous number
2 of guidance pieces and other pieces that basically set
3 out the same methodology that the Commission is
4 following in deciding reasonableness, with one
5 exception, and the exception is that the Commission's
6 process as to the calculation of the potential consumer
7 harm from unauthorized disclosure of information.

8 JUDGE CHAPPELL: Is there a rulemaking going on
9 at this time or are there rules that have been issued in
10 this area?

11 MR. SHEER: There are no -- there is no
12 rulemaking, and no rules have been issued, other than
13 the rule issued with regard to the Gramm-Leach-Bliley
14 Act. There is a safeguards rule there which is issued
15 for financial institutions. The way that rule reads and
16 the way it works, it basically --

17 JUDGE CHAPPELL: The FTC has jurisdiction in
18 that area?

19 MR. SHEER: It has jurisdiction over certain
20 types of financial institutions, such as --

21 JUDGE CHAPPELL: Is that expressed in that Act?

22 MR. SHEER: It is.

23 JUDGE CHAPPELL: Okay.

24 MR. SHEER: As I was saying, Your Honor,
25 information security, which is an essential part of our

1 economy now given the increasing reliance on and use of
2 computer networks, is one of the new areas that the
3 Commission is able to look into. The complaint alleges
4 that the company, LabMD, engaged in an unfair act or
5 practice in violation of Section 5 by collecting and
6 storing large amounts of very sensitive consumer
7 information and failing to use reasonable and
8 appropriate security measures to prevent the information
9 from being disclosed without authorization.

10 As set out in 15 USC 45(n), an act or practice
11 is unfair when it causes or is likely to cause
12 substantial consumer injury that is not -- and the
13 injury is not reasonably avoidable by consumers and not
14 offset by countervailing benefits to consumers or
15 competition. The complaint alleges that LabMD
16 systematically failed to practice what IT professionals
17 generally call -- quote unquote -- defense in depth.

18 Defense in depth is a general approach for
19 identifying the kinds of security measures that will be
20 reasonable under particular circumstances. It sets out
21 guiding principles that IT professionals and industry
22 have known and used for years. There are lots of
23 sources for the principles, such as materials published
24 by the National Institute of Standards and Technology,
25 continuing education for IT professionals, practical IT

1 experience, and lessons learned from publicized
2 breaches.

3 Some of these guiding principles are, first, do
4 not put all your eggs in one basket, because a single
5 security measure may fail or be vulnerable. For
6 example, if the only security measure for a company's
7 network were a firewall and the firewall were not set up
8 correctly, an outsider could exploit the mistake and
9 gain entry to the network, because there are no other
10 security measures in place. The outsider would have
11 free reign within the network and could find -- easily
12 find and export sensitive information.

13 Second, limit a computer user's control over the
14 computers and data to the lowest level the user needs to
15 perform their job. For example, users do not need to be
16 able to change security settings on their computers or
17 install programs on their computers without getting
18 prior approval.

19 Third, also use nontechnical measures, such as
20 providing security training for employees, a plan for
21 responding to security incidents, and maintaining
22 written security policies and procedures for IT
23 employees to follow.

24 The final step in identifying measures that will
25 provide reasonable defense in depth is a common sense

13	<p>1 balancing of the costs and benefits of available 2 security measures. The balancing process is very 3 similar to how businesses decide sometimes whether to 4 purchase new equipment, except that it includes the 5 potential loss from disclosing the company's business 6 plans, for example. This is called risk management, 7 management by IT professionals and industry. 8 The Commission's cases set out this same 9 approach for analyzing the reasonableness of security 10 measures with one possible difference. The possible 11 difference is that the Commission's approach takes into 12 account potential consumer harm from unauthorized 13 disclosure of the information. 14 So, you might ask, how hard is it to do this? 15 In many instances, it will be relatively easy to 16 qualitatively balance cost and benefit using risk 17 management concepts. Consider the following 18 hypothetical. A company uses a program to store 19 thousands of consumer names and Social Security numbers. 20 A vulnerability in the program was discovered and made 21 public a year ago. At the time, IT professionals 22 classified the vulnerability as a 10 risk on a scale of 23 1 to 10, with 10 being the most critical risk. 24 In less than an hour, an IT employee could fix 25 the vulnerability by installing a free update that was</p>	15	<p>1 implement a comprehensive information security program. 2 LabMD systematically failed to use reasonable 3 security measures to protect very sensitive information. 4 I'd like to talk about two of them in a little more 5 depth. The first is the company's failure to use 6 appropriate measures to prevent and detect unauthorized 7 access to consumer information, as happened here when a 8 LabMD file was shared through a peer-to-peer 9 file-sharing network without alarm bells going at off 10 the company. The network is called peer-to-peer, or 11 P2P, because users can share files directly from their 12 own computers to the computers of other people on the 13 network. 14 The complaint alleges in paragraph 18 that a P2P 15 program called Limewire was installed on a LabMD 16 computer used by the company's billing manager. 17 Limewire allows users, like the billing manager, to 18 select files on their computers to make available to 19 other Limewire users. Hundreds of files on the billing 20 manager's computer were available through Limewire, 21 including some business files. 22 One business file that was available and shared 23 contained highly sensitive information about 24 approximately 9300 consumers, including their names, 25 Social Security numbers, dates of birth, health</p>
14	<p>1 made available when the vulnerability was first 2 discovered, and the company didn't do so. The potential 3 loss is very high for this hypothetical. The 4 vulnerability is critical, and disclosing names and 5 Social Security numbers could cause considerable 6 consumer harm. On the other hand, the cost to having an 7 IT professional install the free update is very low. 8 Because the potential consumer loss obviously far 9 exceeds the cost of installing the update, it's 10 unreasonable not to do so. 11 Applying these concepts, LabMD did not pass 12 Defense in Depth 101, not just in one way, but in a 13 number of ways. As set out in paragraph 10 of the 14 complaint, the company failed to identify commonly known 15 or reasonably foreseeable risks to personal information. 16 It did not adequately train employees about security 17 risks and practices. It did not appropriately limit 18 employee access to just the information they needed to 19 do their jobs. 20 It did not correctly or appropriately 21 authenticate users to verify that they are who they say 22 they are. It did not adequately update computer 23 operating systems and equipment. And it did not take 24 reasonable measures to prevent and detect unauthorized 25 access to personal information. And finally, it did not</p>	16	<p>1 insurance provider names and policy numbers, and 2 standardized medical treatment codes. This is the kind 3 of information that can easily be misused to conduct new 4 account fraud and medical identity theft and disclosing 5 treatment codes that may cause privacy harms. 6 Limewire does present a risk that files that 7 should not be shared will be shared inadvertently with 8 other Limewire users, as likely happened here. The 9 irony is that LabMD had no need to accept this risk, 10 because it admittedly had no need for Limewire. The 11 company could have addressed the risk very easily, but 12 it didn't. If it had, it could have stopped Limewire 13 from being downloaded; it could have prevented or 14 detected its installation on the LabMD computer; and it 15 would have been alerted when files were shared so that 16 it could stop the sharing. 17 It's no excuse here that the billing manager 18 should not have been using Limewire in the first place. 19 People are known to make mistakes and to use programs 20 that they shouldn't, which is why technical security 21 measures or controls are needed to achieve defense in 22 depth. 23 JUDGE CHAPPELL: Limewire, is this something 24 that is free or was it purchased? 25 MR. SHEER: Our understanding is that it was</p>

17

1 free.
 2 I'd like to turn to the second failure, and that
 3 is the failure to use appropriate measures to identify
 4 commonly known or reasonably foreseeable risks to
 5 personal information as set out in paragraph 10 of the
 6 complaint. Because no single tool can identify all the
 7 different security threats a company may face, IT
 8 professionals tell us that identifying risks usually
 9 requires a variety of measures or tools.
 10 One such tool that's familiar to almost all of
 11 us is an antivirus program. Another tool is called a
 12 penetration test, which usually includes an automated
 13 vulnerability scan and related activities. Pen tests,
 14 as they're called, probe a company's defenses from the
 15 outside looking for cracks, just like an intruder would.
 16 A pen test might, again, by looking for a
 17 vulnerability in a firewall, looking to test the
 18 firewall for a vulnerability, looking for an opening,
 19 basically, to get into the network. Once inside the
 20 network, the test might test computers and applications
 21 or programs, looking for vulnerabilities that could be
 22 leveraged to get access to sensitive information.
 23 We are told that antivirus programs can't
 24 identify holes in firewalls and that pen tests can't
 25 identify viruses. Both of them are needed to

18

1 effectively identify risks in networks that connect
 2 online like LabMD's. Both are basic, foundational tools
 3 that have been used by companies for years.
 4 JUDGE CHAPPELL: You're talking about antivirus,
 5 but if you have a P2P program, you've created the hole.
 6 So, how is your antivirus going to stop something that
 7 you've created? What's the point of that?
 8 MR. SHEER: That's exactly the point. The point
 9 is that the antivirus program is not going to identify
 10 the P2P application or program that's on your network.
 11 JUDGE CHAPPELL: It's like clicking on the link
 12 on the email you shouldn't open. Your Norton Antivirus
 13 isn't going to stop that because you clicked.
 14 MR. SHEER: You're preaching to the choir, yes.
 15 JUDGE CHAPPELL: Well, not necessarily. I'm
 16 objective here. My point is, why would I pay for extra
 17 antivirus software if I've decided to use P2P software
 18 and I know the hole is there? What's the point in
 19 telling me I needed to put antivirus on my computer?
 20 MR. SHEER: Well, we're not making the argument
 21 that they should have been putting an antivirus on their
 22 computers, and I will say -- and I thought this was what
 23 you said earlier -- that an antivirus program is not
 24 going to identify a P2P program, because it's looking
 25 for viruses, which are small, malicious programs that

19

1 operate in the background that you don't know about,
 2 that you may get on your computer by what you just
 3 described, media that comes in with a link that says
 4 "Click on this link," you click on the link, and a
 5 program -- a virus program is downloaded onto your
 6 computer and operates in the background. But that's not
 7 what we're alleging here was the problem in this
 8 explanation.
 9 What we're alleging here was the failure to have
 10 a penetration test would not identify to the company
 11 other risks that could not be identified by an antivirus
 12 program. That's why the IT professionals tell us that
 13 you really need to have a variety of tools to identify
 14 risks, because there's no one tool that will identify
 15 all the threats that a company faces.
 16 JUDGE CHAPPELL: Okay. Now I follow why you're
 17 talking about antivirus. Go ahead.
 18 MR. SHEER: The complaint alleges that LabMD did
 19 not use adequate measures, such as pen tests, to
 20 identify commonly known or reasonably foreseeable risks.
 21 As a result, it was blind to some risks and, therefore,
 22 unlikely to effectively guard against them.
 23 To sum up, the complaint alleges that LabMD's
 24 security failures went beyond sharing a file with
 25 sensitive information about 9300 people to a P2P

20

1 network. The company's security practices created
 2 vulnerabilities an outsider could stitch together to
 3 find a way into the network, to move around the network
 4 and explore it, to find sensitive information, and then
 5 to package up the information and export it from the
 6 network without the company's noticing.
 7 LabMD failed to implement reasonable security
 8 measures, and that is an unfair act or practice because
 9 it caused or is likely to cause substantial consumer
 10 injury that's not offset by countervailing benefits to
 11 consumers or competition and also not reasonably
 12 avoidable by consumers. After all, how can a consumer
 13 even know what LabMD's security practices were, let
 14 alone assess how adequate or inadequate they might be?
 15 One final point. Neither the complaint nor the
 16 notice order prescribes specific security practices that
 17 LabMD should implement going forward. They do not, for
 18 example, require that a certain vulnerability scanning
 19 product be used. Because security threats and responses
 20 change so rapidly, the order leaves it to the company to
 21 determine the particular security measures that, taken
 22 together, will provide reasonable security at lowest
 23 cost in its circumstances.
 24 Although the Commission retains the right to do
 25 so, under the notice order and all of the other

21

1 Commission information security consent orders, a strong
2 indication that security is reasonable is a security
3 certification from an independent IT professional who's
4 capable of balancing the costs and benefits and follows
5 protocols commonly used in the profession. These are
6 the same sorts of things that internal IT employees
7 commonly do for companies across the country. Frankly,
8 the order only asks LabMD to do what it should have been
9 doing anyway but didn't.

10 Thank you.

11 JUDGE CHAPPELL: I have one question. I heard
12 you refer to Section 5, but I also heard you refer to
13 various other rules, regulations, et cetera. Is it the
14 Government's position that whatever rule or regulation
15 or statute that you're alleging was violated is
16 contained within the four corners of this complaint?

17 MR. SHEER: What we're saying is that the
18 allegation is that the company failed to comply with
19 Section 5 in engaging an unfair act or practice by
20 failing to provide reasonable security for sensitive
21 information. We are saying that reasonableness is a
22 common sense balancing of cost and benefit and that
23 common sense is available from many, many sources,
24 including organizations -- government organizations,
25 such as the National Institute of Standards and

22

1 Technology, private entities, such as the SANS
2 Institute, and many others as well. So that we are
3 assessing reasonable -- reasonableness in much the same
4 way, following the same process that is commonly used
5 throughout the IT industry now. We add only one
6 additional factor, and that is take into account the
7 potential consumer harm from failing to have reasonable
8 security to protect that information.

9 JUDGE CHAPPELL: I'm not sure you answered my
10 question, Counselor. Are there any rules or regulations
11 that you're going to allege were violated here that are
12 not within the four corners of the complaint?

13 MR. SHEER: I misunderstood. I'm sorry. No.

14 JUDGE CHAPPELL: All right. Thank you.

15 MR. RUBINSTEIN: The facts in this case are
16 pretty simple and pretty clear. The billing manager,
17 the person responsible for handling LabMD's invoicing --
18 a small company, a very limited staff --

19 JUDGE CHAPPELL: Tell me more about what LabMD
20 does. Do you take blood samples?

21 MR. RUBINSTEIN: It's a pathology lab. The
22 customers -- LabMD's customers are doctors. You go in
23 to see a doctor -- and it's a very small specialty
24 business for particular kinds of cancer detection. You
25 go in to see a doctor. He will take a tissue sample for

23

1 biopsy or what have you. They don't do the work in the
2 lab, they send it out, and LabMD's market, which is
3 primarily Georgia and the states surrounding it, it
4 would do biopsies and give diagnoses to help with cancer
5 treatment.

6 JUDGE CHAPPELL: So, that work is actually done
7 in your company offices.

8 MR. RUBINSTEIN: That's correct.

9 JUDGE CHAPPELL: You have got the guys in the
10 white lab coats.

11 MR. RUBINSTEIN: That's correct.

12 JUDGE CHAPPELL: Are you doing blood tests, like
13 cholesterol?

14 MR. RUBINSTEIN: No. No, it's only -- and I
15 don't want to speculate, and we will put this in
16 obviously in the facts, but it's related to cancer
17 diagnoses, but only certain kinds of cancers, prostate
18 cancers, other sort of related maladies.

19 JUDGE CHAPPELL: So, generally a doctor takes a
20 biopsy; they send it to you.

21 MR. RUBINSTEIN: That's correct.

22 JUDGE CHAPPELL: Okay.

23 MR. RUBINSTEIN: So, the doctors are our
24 customers, technically.

25 JUDGE CHAPPELL: And the doctor sends the

24

1 patient data to you? Where does the data come from
2 that's alleged to have been released in this case?

3 MR. RUBINSTEIN: The data came from an internal
4 spreadsheet that was used by the billing manager, as I
5 understand it -- as we understand it, to keep track of
6 the accounts. She was in charge of making sure that the
7 insurance companies got billed for the work that LabMD
8 was doing. It was an internal spreadsheet. It was
9 never meant to be shared with anybody.

10 And actually, I would like to, if I could, just
11 take issue with the file that triggered this
12 investigation was not shared; it was stolen. A company
13 called Tiversa, under a government contract --

14 JUDGE CHAPPELL: Wait. I'd like to make sure I
15 understand the particulars, to get a grasp of the big
16 picture.

17 MR. RUBINSTEIN: Yes, sir.

18 JUDGE CHAPPELL: Somebody like INOVA Fairfax
19 sends their tissue samples to your lab, and they
20 probably have patient identifiable information on them,
21 but then someone in your office developed a spreadsheet
22 on their own, nothing to do with INOVA or Johns Hopkins
23 or any other hospital. That was done internally, this
24 spreadsheet.

25 MR. RUBINSTEIN: The spreadsheets were done

25

1 internally using information that came from the doctors.
 2 JUDGE CHAPPELL: Right. But the doctors and the
 3 hospitals knew nothing about it.
 4 MR. RUBINSTEIN: Well, I mean, I assume that
 5 they -- I don't know what they knew to begin with, but
 6 I'm going to assume they knew for billing purposes and
 7 invoicing we had to have some sort of billing procedures
 8 that --
 9 JUDGE CHAPPELL: That's what I was going to ask
 10 you. Why was the spreadsheet created?
 11 MR. RUBINSTEIN: To manage accounts, basically,
 12 accounts receivable.
 13 JUDGE CHAPPELL: And that spreadsheet had
 14 personally identifiable information?
 15 MR. RUBINSTEIN: Sure. It would identify the
 16 individual, their identifying number, and their
 17 insurance information, so that appropriate bills could
 18 be sent out.
 19 JUDGE CHAPPELL: And did your client bill, for
 20 example, Blue Cross or did they bill the hospital or
 21 doctor who sent the sample?
 22 MR. RUBINSTEIN: I think it differed from
 23 patient to patient depending on the particular
 24 circumstances, but I'm not 100 percent sure exactly, you
 25 know, what happened for each patient.

26

1 JUDGE CHAPPELL: It just -- you know, I find it
 2 helps to have a thorough understanding of the business
 3 to then go to an interpretation of what's going on and
 4 what -- and what has happened and what's not.
 5 MR. RUBINSTEIN: Absolutely, Your Honor. It was
 6 standard kind of accounts receivable, is the best way to
 7 conceptualize what this spreadsheet was, and it was a
 8 way internally of tracking who it was and what was being
 9 paid and so forth.
 10 And as I said, there are a couple of things here
 11 from a factual standpoint they are real simple and
 12 clear. The billing manager, she was in charge of -- as,
 13 you know, the proofs will show, she was in charge of
 14 managing money coming in, going out, and so forth,
 15 downloaded Limewire. Limewire is a P2P program that was
 16 primarily, I think, designed to share music and other
 17 files.
 18 A government contractor by the time of Tiversa
 19 was paid, in conjunction with Professor Eric Johnson to
 20 surveil other companies --
 21 JUDGE CHAPPELL: How do you spell that?
 22 MR. RUBINSTEIN: Tiversa?
 23 JUDGE CHAPPELL: Yes.
 24 MR. RUBINSTEIN: T-I-V, Victor, E-R-S, as in
 25 Sam, -A.

27

1 JUDGE CHAPPELL: Is that like an incorporated
 2 company or --
 3 MR. RUBINSTEIN: It's a security -- an internet
 4 security company based in Pittsburgh, a pretty large
 5 company. And apparently they had contracts with several
 6 government agencies to go out and see -- knock on doors,
 7 as if it were, and see if they could log in and steal
 8 files, and they did. And they put out a press release,
 9 Tiversa, that is --
 10 JUDGE CHAPPELL: And just so you know, this is
 11 not argument. You are telling me what you're going to
 12 prove at trial.
 13 MR. RUBINSTEIN: This is what's going to be
 14 proven, talking about right now the facts. They put out
 15 a press release claiming that they had found all sorts
 16 of breaches with spreadsheets that contained client
 17 names, Social Security numbers, birth dates, detailed
 18 hospital databases, over 20,000 patients, and the press
 19 release mentions the file that was taken from LabMD in
 20 this case.
 21 The proofs will show that Tiversa notified the
 22 Respondent that it obtained one or stole one of LabMD's
 23 files --
 24 JUDGE CHAPPELL: Let me make sure I understand
 25 this. You're saying Tiversa had a contract, they were

28

1 paid by our Government, to try to break in or hack
 2 files?
 3 MR. RUBINSTEIN: Yes, sir. There was a study
 4 done by this Professor Eric Johnson in conjunction with
 5 Tiversa. I believe that the study was funded, according
 6 to Tiversa, by the Department of Homeland Security,
 7 among others. Yeah, it was designed to test the
 8 security of networks for confidential health and other
 9 information. And we will put into evidence --
 10 JUDGE CHAPPELL: Are you aware of the details of
 11 that contract?
 12 MR. RUBINSTEIN: We don't have a copy of the
 13 contract yet. We are going to get it in discovery we
 14 hope.
 15 JUDGE CHAPPELL: For example, if you're a victim
 16 of the hacking, do they inform you and do they tell you
 17 what's been done?
 18 MR. RUBINSTEIN: Well, that's what they did in
 19 this case, and then the testimony, certainly from
 20 LabMD's principals, is going to be that they then
 21 pitched their business. LabMD turned them down and
 22 said, "No, thank you," at which point in time the -- the
 23 stolen file made its way to the Government, and this
 24 proceeding followed.
 25 So, we don't know at what point in time Tiversa

29	<p>1 and the Government began communicating about LabMD. We</p> <p>2 anticipate that that relationship will be clarified in</p> <p>3 discovery, and it's obviously something we're very</p> <p>4 interested in.</p> <p>5 JUDGE CHAPPELL: All right. You're saying you</p> <p>6 have proof, they told you you were hacked, they wanted</p> <p>7 to charge you to prevent attacks, but you're assuming</p> <p>8 they then spread the infor -- spread the data out.</p> <p>9 MR. RUBINSTEIN: Well, as far as we know --</p> <p>10 JUDGE CHAPPELL: Are you making a jump there or</p> <p>11 do you have proof of that?</p> <p>12 MR. RUBINSTEIN: No, we believe -- we have proof</p> <p>13 of that. That's how the file came to the FTC, was from</p> <p>14 Tiversa. And, in fact, there will be testimony that a</p> <p>15 lawyer for Tiversa called a lawyer for LabMD, I think</p> <p>16 about a 12-, 13-month time frame, and said, "Well, we're</p> <p>17 giving this document now to the Government."</p> <p>18 JUDGE CHAPPELL: Did you get any complaints from</p> <p>19 customers, your clients?</p> <p>20 MR. RUBINSTEIN: No, sir. To the best of our</p> <p>21 knowledge, this file -- the only entities that have seen</p> <p>22 this, other than LabMD and its employees, are Tiversa</p> <p>23 and the Government.</p> <p>24 JUDGE CHAPPELL: So, it's your position this</p> <p>25 information hasn't been released.</p>	31	<p>1 JUDGE CHAPPELL: Well, that's my job. I am</p> <p>2 going to deal with the fundamental disagreement.</p> <p>3 MR. SHEER: Our view -- and we will put on</p> <p>4 evidence that shows this -- is that Limewire -- is that</p> <p>5 the LabMD file was not taken by being stolen; instead,</p> <p>6 Limewire does two things, basically two things. Someone</p> <p>7 installs it on their computer. It allows them to</p> <p>8 designate files on their computer that they will make</p> <p>9 freely available to anybody else on the Limewire</p> <p>10 network.</p> <p>11 JUDGE CHAPPELL: I understand how P2P works. I</p> <p>12 may not look like it, but I understand technology.</p> <p>13 MR. SHEER: Okay.</p> <p>14 JUDGE CHAPPELL: What I want to know is what's</p> <p>15 your position of what happened to this actual data</p> <p>16 that's in dispute here or the subject of this dispute?</p> <p>17 MR. SHEER: Our position is that the information</p> <p>18 was actually shared voluntarily from LabMD by virtue of</p> <p>19 its being in the "my shared files" folder in Limewire on</p> <p>20 the computer.</p> <p>21 JUDGE CHAPPELL: And you have a witness who's</p> <p>22 going to say, "I saw it, they shared it with me"?</p> <p>23 MR. SHEER: We have evidence that will show that</p> <p>24 the file that is in issue was, in fact, in the "my</p> <p>25 shared files" folder.</p>
30	<p>1 MR. RUBINSTEIN: That's correct. What we're</p> <p>2 also not clear, though, I should say, because this is --</p> <p>3 as I mentioned, Tiversa puts out a press release</p> <p>4 identifying a number of other companies for which it</p> <p>5 attained data. It's not clear to us what happened to</p> <p>6 that data, where it went, whether it came to the</p> <p>7 Government, how the decision was made or why the</p> <p>8 decision was made to disclose LabMD's data. And,</p> <p>9 obviously, that -- all of those issues, we believe, are</p> <p>10 very significant and have very immediate, clear legal</p> <p>11 consequences. And so they are going to be addressed in</p> <p>12 discovery.</p> <p>13 We also are, frankly, going to investigate why</p> <p>14 the Government knowingly commenced an investigation</p> <p>15 using a stolen file obtained from a government</p> <p>16 contractor being paid with taxpayer money to steal from</p> <p>17 LabMD. It doesn't make sense to us.</p> <p>18 There are a number of very significant legal</p> <p>19 issues --</p> <p>20 JUDGE CHAPPELL: Hold on a second.</p> <p>21 Mr. Sheer, what's the Government's position on</p> <p>22 the disclosure of the data?</p> <p>23 MR. SHEER: This comes down to a fundamental</p> <p>24 disagreement about how Limewire and other P2P</p> <p>25 applications work.</p>	32	<p>1 JUDGE CHAPPELL: That it was available to be</p> <p>2 viewed.</p> <p>3 MR. SHEER: Correct. It was available to anyone</p> <p>4 who might look for it using Limewire.</p> <p>5 JUDGE CHAPPELL: Kind of like when the</p> <p>6 Commission posted proprietary data a few years in a case</p> <p>7 that fortunately was not mine; there was this assumption</p> <p>8 that nobody had seen it, but now the assumption is</p> <p>9 somebody did see it?</p> <p>10 MR. SHEER: Well, we know it was downloaded by</p> <p>11 one entity, they're saying Tiversa, and we also -- we</p> <p>12 also know that, because it was available, it could have</p> <p>13 been downloaded by any number of other people. And one</p> <p>14 would also want to say, even if you accept all of</p> <p>15 that -- which we don't -- it would have been very easy</p> <p>16 for the company to prevent this from having happened in</p> <p>17 the first place.</p> <p>18 JUDGE CHAPPELL: And, again, I'm not -- clearly</p> <p>19 not making any substantive decisions today, but I'm just</p> <p>20 trying to figure out what the positions are, when I hear</p> <p>21 something this 180 degrees different. So, what you're</p> <p>22 telling me, though, is you're not going to have a</p> <p>23 witness say they saw it, but you intend to prove that it</p> <p>24 was available publicly.</p> <p>25 MR. SHEER: We will be able to show that it was</p>

1 available publicly and we may be able to have a witness
 2 who says they saw it.
 3 JUDGE CHAPPELL: Do you have any complaining
 4 witnesses who say their data was released or disclosed?
 5 MR. SHEER: Not at this time.
 6 JUDGE CHAPPELL: Okay.
 7 MR. SHEER: We will develop that.
 8 JUDGE CHAPPELL: All right. Thank you.
 9 MR. RUBINSTEIN: There are some very significant
 10 legal issues that are created by these facts. The first
 11 is the ambit of the Commission's authority under Section
 12 5, which we intend to test. The second is the extent to
 13 which the file in question is within the Commission's
 14 ambit under Article 1, Section 8. There are due process
 15 issues, because notwithstanding counsel's discussions,
 16 there are no fixed or ascertainable standards by which
 17 LabMD, a small company, could judge the propriety of
 18 what it was doing.
 19 Proofs will show that the billing manager
 20 downloaded Limewire and did it without the knowledge of
 21 the company's upper management and contrary to the
 22 company policy. This was not a shared file. This was
 23 not a shared file at all. It was never meant for public
 24 consumption. In fact, there's yet another issue here.
 25 LabMD is subject to HIPAA, and the Department of Health

1 and Human Services determined that no action was
 2 appropriate.
 3 So, in effect, you have the Commission
 4 overfiling the agency of the Government that Congress
 5 designated with primary responsibility for management
 6 and regulation of HIPAA.
 7 JUDGE CHAPPELL: So, you're saying -- your
 8 position is the data was not in a shared folder.
 9 MR. RUBINSTEIN: It may have been in a -- it was
 10 in a folder and obviously it was accessible to Tiversa.
 11 The mechanics of how Tiversa accessed it and what kind
 12 of folder it was in are things that we are not clear
 13 about and we are going to, through discovery, better
 14 ascertain.
 15 Certainly, it was not supposed to be made
 16 available to the public. That was not LabMD's policy,
 17 certainly, and to the extent that the Limewire was
 18 downloaded, it was done, as I said, without
 19 authorization and contrary to LabMD's standard policies.
 20 JUDGE CHAPPELL: I've heard you say a couple
 21 times you're a small company. I mean, is that
 22 confidential? I mean, are you 5 million, 10 million?
 23 What kind of revenues? If it's not -- just ballpark.
 24 How small or how large are you.
 25 MR. RUBINSTEIN: I would rather not -- I will

1 make that information available to you in camera.
 2 JUDGE CHAPPELL: That's okay. I'll see it in
 3 the documents. I just thought, when you say small, you
 4 know --
 5 MR. RUBINSTEIN: I would rather not -- we will
 6 say it is a small company with less than 50 employees,
 7 is my understanding. We will make that available to
 8 you, Your Honor.
 9 JUDGE CHAPPELL: Less than 50, 5-0, or 15?
 10 MR. RUBINSTEIN: I'm sorry, less than 50. But
 11 for various reasons, it's a closely held corporation,
 12 and I don't want to put the numbers out. But we are not
 13 INOVA or Johns Hopkins.
 14 JUDGE CHAPPELL: Labcorp?
 15 MR. RUBINSTEIN: Not them either.
 16 So, what we anticipate with this case, as I
 17 said, we are going to have to find out Tiversa's role.
 18 We are going to have to find out the extent to which it
 19 was involved with and its relationship with the
 20 Commission in the decision to move forward with this
 21 investigation. And we're going to be filing a series of
 22 dispositive motions very early on, because quite
 23 frankly, we don't believe the Commission has the
 24 authority to be doing what it's doing to LabMD. We
 25 don't think that the information --

1 JUDGE CHAPPELL: Very early on?
 2 MR. RUBINSTEIN: Very early on, within the -- I
 3 mentioned this to counsel. We anticipate filing a
 4 series of motions within the next two to three weeks.
 5 JUDGE CHAPPELL: And you understand who will be
 6 deciding those motions?
 7 MR. RUBINSTEIN: We are well aware, Your Honor,
 8 but we have an obligation to exhaust our remedies. So,
 9 we're going to be raising a series of legal issues.
 10 We're going to be raising a series of evidentiary
 11 objections based on the circumstances, as we understand
 12 them today, about how the Government came into
 13 possession of the information in the first instance.
 14 And then all of the other things that are laid
 15 out in the complaint were the result of the knowing
 16 acceptance from a government contractor of a stolen
 17 file, files stolen, by the way, in contravention of
 18 Georgia's law. There was a case in the Eleventh Circuit
 19 which was dismissed for want of jurisdiction under the
 20 Georgia long arm statute, but there is, you know, a
 21 clear suggestion that what Tiversa did violate Georgia's
 22 law.
 23 JUDGE CHAPPELL: Who brought that case?
 24 MR. RUBINSTEIN: LabMD against Tiversa.
 25 JUDGE CHAPPELL: And, of course, LabMD didn't

37

1 decide that motion, did they?

2 MR. RUBINSTEIN: Well, it was dismissed based
3 on, like I said, lack of long arm jurisdiction. I have
4 a copy of the Eleventh Circuit decision if you would
5 like it. I can provide that to you right now, if you
6 care to see it.

7 JUDGE CHAPPELL: It won't do me any good until
8 after the hearing starts.

9 MR. RUBINSTEIN: But that's where we're at.
10 We're going to be filing dispositive motions. We fully
11 anticipate that the scope of discovery will be
12 clarified. We look forward to working with the
13 Government to ensure that this matter moves as quickly
14 and as painlessly forward as possible. And we look
15 forward to trying this issue before Your Honor.

16 JUDGE CHAPPELL: Anything else?

17 MR. RUBINSTEIN: I believe, for today, that's --
18 that's enough.

19 JUDGE CHAPPELL: I notice there's another
20 attorney who's appeared in the case for your client.
21 Are you -- can you let us know, is he going to be 50/50?
22 Is he going to be involved in taking witnesses?

23 MR. RUBINSTEIN: Yes, Your Honor. And forgive
24 me, I should have explained this up front. LabMD is
25 represented by Cause of Action, a 501(C)(3) charity that

38

1 does government accountability, government watchdog, and
2 government transparency work. In the interest of their
3 educational mission, they from time to time take on
4 lawsuits that implicate important issues. In this case,
5 there's an organizational issue in the fact that you
6 have a government commission acting and putting in
7 jeopardy a small business without having any clear
8 standards or ascertainable standards for doing so.

9 So, I'm a partner at Dinsmore & Shohl. I have a
10 practice. Cause of Action is a client of mine from time
11 to time. They asked me to serve as lead counsel. There
12 will be a staff counsel from Cause of Action by the name
13 of Michael Pepson who will be involved in this case. A
14 lot of the document production and so forth that we will
15 be doing will be coming from Cause of Action, but I will
16 be serving as lead counsel and he will be assisting me.

17 JUDGE CHAPPELL: All right, thank you.

18 MR. RUBINSTEIN: Thank you.

19 JUDGE CHAPPELL: Mr. Sheer, anything further?

20 MR. SHEER: No, Your Honor.

21 JUDGE CHAPPELL: Okay. Hearing nothing further,
22 we are, until we meet again, adjourned.

23 (Whereupon, at 2:46 p.m., the initial pretrial
24 conference was adjourned.)
25

39

1 CERTIFICATION OF REPORTER

2 DOCKET/FILE NUMBER: DOCKET 9357

3 CASE TITLE: IN RE: LABMD, INC.

4 DATE: SEPTEMBER 25, 2013

5
6 I HEREBY CERTIFY that the transcript contained
7 herein is a full and accurate transcript of the notes
8 taken by me at the hearing on the above cause before the
9 FEDERAL TRADE COMMISSION to the best of my knowledge and
10 belief.

11
12 DATED: 9/25/2013

13
14
15
16 SUSANNE BERGLING, RMR-CRR-CLR

17
18 CERTIFICATION OF PROOFREADER

19
20 I HEREBY CERTIFY that I proofread the transcript
21 for accuracy in spelling, hyphenation, punctuation and
22 format.

23
24
25 SARA J. VANCE, CMRS

<p style="text-align: center;">A</p> <p>able 11:3 12:16 32:25 33:1</p> <p>Absolutely 26:5</p> <p>accept 16:9 32:14</p> <p>acceptance 36:16</p> <p>access 8:22 14:18,25 15:7 17:22</p> <p>accessed 34:11</p> <p>accessible 34:10</p> <p>accommodation 4:19</p> <p>account 8:16 13:12 16:4 22:6</p> <p>accountability 38:1</p> <p>accounts 9:3 24:6 25:11,12 26:6</p> <p>accuracy 39:21</p> <p>accurate 39:7</p> <p>achieve 16:21</p> <p>act 9:10 10:14,21 11:4,10 20:8 21:19</p> <p>acting 38:6</p> <p>action 9:9 34:1 37:25 38:10,12,15</p> <p>activities 17:13</p> <p>actual 31:15</p> <p>add 8:9 22:5</p> <p>addition 9:23,25</p> <p>additional 22:6</p> <p>address 9:11</p> <p>addressed 16:11 30:11</p> <p>adequate 19:19 20:14</p> <p>adequately 14:16,22</p> <p>adjourned 38:22,24</p> <p>Administrative 2:20</p> <p>admittedly 16:10</p> <p>afternoon 4:10,12</p> <p>agencies 27:6</p> <p>agency 34:4</p> <p>ago 7:25 13:21</p> <p>agreements 9:19</p> <p>ahead 4:9 8:10 19:17</p>	<p>Alain 3:4 4:11</p> <p>alarm 15:9</p> <p>alerted 16:15</p> <p>allegation 21:18</p> <p>allege 22:11</p> <p>alleged 24:2</p> <p>alleges 11:3,15 15:14 19:18,23</p> <p>alleging 19:7,9 21:15</p> <p>allow 8:5</p> <p>allows 15:17 31:7</p> <p>ambit 33:11,14</p> <p>AMERICA 2:1</p> <p>amount 5:18</p> <p>amounts 11:6</p> <p>analyzing 13:9</p> <p>answered 22:9</p> <p>anticipate 5:19,21 6:23 29:2 35:16 36:3 37:11</p> <p>antivirus 17:11,23 18:4,6,9,12,17,19 18:21,23 19:11,17</p> <p>anybody 24:9 31:9</p> <p>anyway 21:9</p> <p>apparently 27:5</p> <p>appearances 3:1 4:8</p> <p>appeared 37:20</p> <p>application 18:10</p> <p>applications 17:20 30:25</p> <p>Applying 14:11</p> <p>appreciated 4:20</p> <p>approach 11:18 13:9,11</p> <p>appropriate 8:23 11:8 15:6 17:3 25:17 34:2</p> <p>appropriately 14:17 14:20</p> <p>approval 12:18</p> <p>approximately 6:3 15:24</p> <p>area 10:10,18</p> <p>areas 9:12 11:2</p> <p>argument 18:20</p>	<p>27:11</p> <p>arm 36:20 37:3</p> <p>Arthaud 3:25</p> <p>Article 33:14</p> <p>ascertain 34:14</p> <p>ascertainable 33:16 38:8</p> <p>asheer@ftc.gov 3:14</p> <p>asked 38:11</p> <p>asks 21:8</p> <p>assess 20:14</p> <p>assesses 9:22</p> <p>assessing 22:3</p> <p>assistant 5:10</p> <p>assisting 38:16</p> <p>associated 6:25</p> <p>assume 25:4,6</p> <p>assuming 29:7</p> <p>assumption 32:7,8</p> <p>attacks 29:7</p> <p>attained 30:5</p> <p>attorney 37:20</p> <p>authenticate 14:21</p> <p>authority 9:11 33:11 35:24</p> <p>authorization 11:9 34:19</p> <p>automated 17:12</p> <p>available 13:1 14:1 15:18,20,22 21:23 31:9 32:1,3,12,24 33:1 34:16 35:1,7</p> <p>Avenue 3:11,19</p> <p>avoidable 11:13 20:12</p> <p>aware 9:21 28:10 36:7</p> <hr/> <p style="text-align: center;">B</p> <hr/> <p>B 4:4</p> <p>background 19:1,6</p> <p>balance 13:16</p> <p>balancing 13:1,2 21:4,22</p> <p>ballpark 5:22 34:23</p> <p>bank 9:3</p>	<p>based 27:4 36:11 37:2</p> <p>basic 18:2</p> <p>basically 10:2,16 17:19 25:11 31:6</p> <p>basket 12:4</p> <p>began 29:1</p> <p>BEHALF 3:3,16</p> <p>belief 39:10</p> <p>believe 28:5 29:12 30:9 35:23 37:17</p> <p>bells 15:9</p> <p>benefit 13:16 21:22</p> <p>benefits 9:5 11:14 13:1 20:10 21:4</p> <p>Bergling 2:25 39:16</p> <p>best 26:6 29:20 39:9</p> <p>better 34:13</p> <p>beyond 19:24</p> <p>big 24:15</p> <p>bill 25:19,20</p> <p>billed 24:7</p> <p>billing 15:16,17,19 16:17 22:16 24:4 25:6,7 26:12 33:19</p> <p>bills 25:17</p> <p>biopsies 23:4</p> <p>biopsy 23:1,20</p> <p>birth 15:25 27:17</p> <p>blind 19:21</p> <p>blood 8:12 22:20 23:12</p> <p>Blue 25:20</p> <p>body 7:13</p> <p>boundaries 7:5</p> <p>breaches 12:2 27:16</p> <p>break 28:1</p> <p>broad 9:11</p> <p>brought 9:10 36:23</p> <p>business 8:19,20 13:5 15:21,22 22:24 26:2 28:21 38:7</p> <p>businesses 13:3</p> <hr/> <p style="text-align: center;">C</p> <hr/> <p>C 4:1 39:1,1,18,18</p>	<p>calculation 10:6</p> <p>call 4:3 11:17</p> <p>called 13:6 15:10,15 17:11,14 24:13 29:15</p> <p>camera 35:1</p> <p>cancer 22:24 23:4 23:16</p> <p>cancers 23:17,18</p> <p>capable 21:4</p> <p>card 9:3</p> <p>care 37:6</p> <p>case 1:4 7:14 8:6 22:15 24:2 27:20 28:19 32:6 35:16 36:18,23 37:20 38:4,13 39:3</p> <p>cases 13:8</p> <p>cause 11:11 14:5 16:5 20:9 37:25 38:10,12,15 39:8</p> <p>caused 20:9</p> <p>causes 11:11</p> <p>certain 10:19 20:18 23:17</p> <p>certainly 28:19 34:15,17</p> <p>certification 21:3</p> <p>CERTIFY 39:6,20</p> <p>cetera 21:13</p> <p>change 12:16 20:20</p> <p>CHAPPELL 2:19 4:3,7,14,21,24 5:3 6:1,4,9,13,16 7:1 8:3,5,18 9:13 10:8 10:17,21,23 16:23 18:4,11,15 19:16 21:11 22:9,14,19 23:6,9,12,19,22,25 24:14,18 25:2,9,13 25:19 26:1,21,23 27:1,10,24 28:10 28:15 29:5,10,18 29:24 30:20 31:1 31:11,14,21 32:1,5 32:18 33:3,6,8 34:7,20 35:2,9,14</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

36:1,5,23,25 37:7 37:16,19 38:17,19 38:21 charge 24:6 26:12 26:13 29:7 charity 37:25 checking 8:16 choir 18:14 cholesterol 23:13 Circuit 36:18 37:4 circumstances 11:20 20:23 25:24 36:11 claiming 27:15 clarified 29:2 37:12 classified 13:22 clear 22:16 26:12 30:2,5,10 34:12 36:21 38:7 clearly 32:18 click 19:4,4 clicked 18:13 clicking 18:11 client 25:19 27:16 37:20 38:10 clients 29:19 closely 35:11 CMRS 39:25 coats 23:10 codes 16:2,5 collected 8:14 collecting 11:5 come 4:22 24:1 comes 19:3 30:23 coming 26:14 38:15 commenced 30:14 comment 8:3 commission 2:2 3:3 3:9 4:11 7:13,18 7:20 9:11,14,18,21 9:24 10:3 11:3 20:24 21:1 32:6 34:3 35:20,23 38:6 39:9 Commission's 10:5 13:8,11 33:11,13 common 12:25	21:22,23 commonly 14:14 17:4 19:20 21:5,7 22:4 communicating 29:1 communications 5:9 companies 9:14 18:3 21:7 24:7 26:20 30:4 company 9:16,18 11:4 13:18 14:2,14 15:10 16:11 17:7 19:10,15 20:20 21:18 22:18 23:7 24:12 27:2,4,5 32:16 33:17,22 34:21 35:6 company's 12:6 13:5 15:5,16 17:14 20:1,6 33:21 competition 11:15 20:11 complaining 33:3 complaint 4:13 7:14 9:6 11:3,15 14:14 15:14 17:6 19:18 19:23 20:15 21:16 22:12 36:15 complaints 9:7 29:18 comply 21:18 comprehensive 15:1 computer 11:2 12:13 14:22 15:16 15:20 16:14 18:19 19:2,6 31:7,8,20 computers 12:14,16 12:17 15:12,12,18 17:20 18:22 concepts 13:17 14:11 conceptualize 26:7 conduct 9:2 16:3 conference 2:12 38:24 confidential 28:8	34:22 Congress 34:4 conjunction 26:19 28:4 connect 18:1 consent 9:19 21:1 consequences 30:11 Consider 13:17 considerable 14:5 consumer 6:7,12 10:6 11:6,12 13:12 13:19 14:6,8 15:7 20:9,12 22:7 consumers 8:13,15 8:24 11:13,14 15:24 20:11,12 consumption 33:24 contained 15:23 21:16 27:16 39:6 continuing 11:25 contract 24:13 27:25 28:11,13 contractor 26:18 30:16 36:16 contracts 27:5 contrary 33:21 34:19 contravention 36:17 control 12:13 controls 16:21 copies 5:5,6,12 copy 28:12 37:4 corners 21:16 22:12 corporation 2:7 35:11 correct 8:4 23:8,11 23:21 30:1 32:3 correctly 12:8 14:20 cost 13:16 14:6,9 20:23 21:22 costs 13:1 21:4 counsel 4:13,19 36:3 38:11,12,16 counsel's 33:15 Counselor 22:10 countervailing 11:14 20:10	country 21:7 couple 26:10 34:20 course 36:25 courtesy 5:5,6,11 covers 7:9 COX 3:6 cracks 17:15 created 18:5,7 20:1 25:10 33:10 credit 9:3 critical 13:23 14:4 Cross 25:20 current 7:1 customers 22:22,22 23:24 29:19	described 19:3 designate 5:8 31:8 designated 34:5 designed 26:16 28:7 detailed 27:17 details 28:10 detect 14:24 15:6 detected 16:14 detection 22:24 determine 20:21 determined 34:1 develop 7:3 9:12 33:7 developed 24:21 diagnoses 23:4,17 differed 25:22 difference 13:10,11 different 17:7 32:21 Dinsmore 3:18 38:9 directly 15:11 disagreement 30:24 31:2 disclose 30:8 disclosed 11:9 33:4 disclosing 13:5 14:4 16:4 disclosure 10:7 13:13 30:22 discovered 13:20 14:2 discovery 28:13 29:3 30:12 34:13 37:11 discussions 7:21,23 8:1 33:15 dismiss 7:15,18 dismissed 36:19 37:2 dispositive 7:7 35:22 37:10 dispute 31:16,16 Division 3:10 Docket 2:6 4:3 39:2 DOCKET/FILE 39:2 doctor 22:23,25 23:19,25 25:21
D				
D 1:1 2:19 3:17 4:1 39:18 D.C 3:12,20 Dana 5:10 data 12:14 24:1,1,3 29:8 30:5,6,8,22 31:15 32:6 33:4 34:8 databases 27:18 DATE 39:4 DATED 39:12 dates 15:25 27:17 deadline 7:8 deal 5:1 31:2 decide 13:3 37:1 decided 7:20 18:17 deciding 10:4 36:6 decision 30:7,8 35:20 37:4 decisions 32:19 defense 11:17,18 12:25 14:12 16:21 defenses 17:14 degrees 32:21 Department 28:6 33:25 depending 9:1 25:23 depth 11:17,18 12:25 14:12 15:5 16:22				

doctors 8:13 22:22 23:23 25:1,2	equipment 13:4 14:23	failing 8:23 11:7 21:20 22:7	22:4	going 6:4,6 10:8 15:9 18:6,9,13,24 20:17 22:11 25:6,9 26:3,14 27:11,13 28:13,20 30:11,13 31:2,22 32:22 34:13 35:17,18,21 36:9,10 37:10,21 37:22
document 29:17 38:14	Eric 26:19 28:4	failure 15:5 17:2,3 19:9	follows 21:4	good 4:10,12 37:7
documents 35:3	ESQ 3:4,5,6,7,8,17	failures 19:24	foreseeable 14:15 17:4 19:20	government 4:9,19 5:21 8:7 21:24 24:13 26:18 27:6 28:1,23 29:1,17,23 30:7,14,15 34:4 36:12,16 37:13 38:1,1,2,6
doing 8:13 21:9 23:12 24:8 33:18 35:24,24 38:8,15	essential 10:25	Fairfax 24:18	forgive 37:23	Government's 6:22 21:14 30:21
doors 27:6	et 21:13	fairly 6:5	format 39:22	Gramm-Leach-Bl... 10:13
downloaded 16:13 19:5 26:15 32:10 32:13 33:20 34:18	evidence 28:9 31:4 31:23	familiar 17:10	forth 26:9,14 38:14	grasp 24:15
draft 5:14	evidentiary 7:17,19 36:10	far 14:8 29:9	fortunately 32:7	Gross 5:10
due 33:14	exactly 18:8 25:24	Federal 2:2 3:3,9 39:9	forward 20:17 35:20 37:12,14,15	guard 19:22
E	example 9:1 12:6,15 13:6 20:18 25:20 28:15	figure 32:20	found 27:15	guidance 10:2
E 1:1 4:1,1 39:1,1,1 39:18,18,18	exceeds 14:9	file 6:25 7:10 15:8 15:22 19:24 24:11 27:19 28:23 29:13 29:21 30:15 31:5 31:24 33:13,22,23 36:17	foundational 18:2	guidelines 9:14
E-R-S 26:24	exception 10:5,5	file-sharing 15:9	four 21:16 22:12	guiding 11:21 12:3
earlier 18:23	excuse 16:17	filed 7:16,19	frame 29:16	guys 23:9
early 35:22 36:1,2	exhaust 36:8	files 15:11,18,19,21 16:6,15 26:17 27:8 27:23 28:2 31:8,19 31:25 36:17	frankly 21:7 30:13 35:23	H
easily 12:11 16:3,11	expect 4:21 5:24	filing 35:21 36:3 37:10	fraud 9:3 16:4 14:7 16:24 17:1	hack 28:1
easy 13:15 32:15	expecting 6:11	final 12:24 20:15	free 12:11 13:25 14:7 16:24 17:1	hacked 29:6
economy 11:1	experience 12:1	finally 14:25	freely 31:9	hacking 28:16
education 11:25	expert 6:21	financial 9:1 10:15 10:20	Friday 5:16,16	hand 14:6
educational 9:24 38:3	experts 6:5,7,12,12	find 12:11,12 20:3,4 26:1 35:17,18	front 37:24	handling 22:17
effect 34:3	explained 37:24	firewall 12:7,7 17:17,18	FTC 9:6,10 10:17 29:13	happened 15:7 16:8 25:25 26:4 30:5 31:15 32:16
effectively 18:1 19:22	explanation 19:8	firewalls 17:24	full 39:7	hard 13:14
eggs 12:4	exploit 12:8	firms 9:20	fully 37:10	harm 6:24 10:7 13:12 14:6 22:7
eight 5:24	explore 20:4	first 5:13 8:7 12:3 14:1 15:5 16:18 32:17 33:10 36:13	fundamental 30:23 31:2	harms 16:5
either 6:18 35:15	export 12:12 20:5	fix 13:24	funded 28:5	health 15:25 28:8 33:25
Eleventh 36:18 37:4	exposes 8:21	fixed 33:16	further 38:19,21	hear 6:10 32:20
email 5:5,9 18:12	expressed 10:21	folder 31:19,25 34:8 34:10,12	G	heard 21:11,12 34:20
employee 13:24 14:18	extent 33:12 34:17 35:18	follow 4:25 12:23 19:16	G 4:1	
employees 12:20,23 14:16 21:6 29:22 35:6	extra 18:16	followed 28:24	gain 12:9	
engaged 11:4	F	following 10:4 13:17	Gebler 3:25	
engaging 21:19	F 39:1,1,18,18,18		general 11:18 23:19	
ensured 9:18	face 17:7		generally 11:17 23:19	
entities 22:1 29:21	faces 19:15		Georgia 23:3 36:20	
entity 32:11	fact 29:14 31:24 33:24 38:5		Georgia's 36:18,21	
entry 12:9	factor 22:6		getting 5:19 12:17	

hearing 7:2,5,17,19 37:8 38:21 39:8	identity 3:10 8:24 9:5,9 16:4	instance 36:13	21:11 22:9,14,19	11:4,15 14:11 15:2
held 35:11	immediate 30:10	instances 13:15	23:6,9,12,19,22,25	15:8,15 16:9,14
help 23:4	impersonate 8:25	Institute 11:24	24:14,18 25:2,9,13	19:18 20:7,17 21:8
helps 26:2	implement 15:1	21:25 22:2	25:19 26:1,21,23	22:19 24:7 27:19
high 14:3	20:7,17	institutions 10:15	27:1,10,24 28:10	28:21 29:1,15,22
highly 15:23	implicate 38:4	10:20	28:15 29:5,10,18	30:17 31:5,18
Hillary 3:25	important 38:4	insurance 9:4 16:1	29:24 30:20 31:1	33:17,25 35:24
HIPAA 33:25 34:6	inadequate 20:14	24:7 25:17	31:11,14,21 32:1,5	36:24,25 37:24
history 5:13	inadvertently 16:7	intend 7:10 32:23	32:18 33:3,6,8,17	39:3
Hold 30:20	incidents 12:21	33:12	34:7,20 35:2,9,14	LabMD's 18:2
holding 5:22	includes 13:4 17:12	interest 7:24 38:2	36:1,5,23,25 37:7	19:23 20:13 22:17
hole 18:5,18	including 8:15	interested 29:4	37:16,19 38:17,19	22:22 23:2 27:22
holes 17:24	15:21,24 21:24	internal 21:6 24:3,8	38:21	28:20 30:8 34:16
Homeland 28:6	incorporated 27:1	internally 24:23	judgment 7:9,10	34:19
Honor 4:6,10,12,16	increasing 11:1	25:1 26:8	judgments 7:12	laboratory 8:12
4:23 6:6,14 8:4,11	independent 21:3	internet 27:3	jump 29:10	lack 37:3
10:24 26:5 35:8	indicated 7:24	interpretation 26:3	jurisdiction 10:17	laid 36:14
36:7 37:15,23	indication 21:2	intruder 17:15	10:19 36:19 37:3	large 11:6 27:4
38:20	individual 25:16	investigate 30:13		34:24
HONORABLE 2:19	individuals 5:8	investigation 24:12	K	LASSACK 3:7
hope 28:14	industry 9:25 10:1	30:14 35:21	keep 7:4 24:5	latest 5:17
Hopkins 24:22	11:21 13:7 22:5	invoicing 22:17 25:7	kind 16:2 26:6 32:5	Laura 3:5 4:13
35:13	infor 29:8	involved 35:19	34:11,23	law 2:20 36:18,22
hospital 24:23 25:20	inform 28:16	37:22 38:13	kinds 11:19 22:24	lawsuits 38:4
27:18	information 8:14,16	irony 16:9	23:17	lawyer 29:15,15
hospitals 25:3	8:21,25 9:1,2,4,8,9	issue 5:15 7:13	knew 25:3,5,6	lead 38:11,16
hour 13:24	9:15 10:7,25 11:7	24:11 31:24 33:24	knock 27:6	learned 12:1
hours 7:2	11:8 12:12 13:13	37:15 38:5	know 7:11 8:8 18:18	leaves 20:20
Human 34:1	14:15,18,25 15:1,3	issued 9:14 10:1,9	19:1 20:13 25:5,25	legal 30:10,18 33:10
hundreds 8:14,18	15:7,23 16:3 17:5	10:12,13,14	26:1,13 27:10	36:9
15:19	17:22 19:25 20:4,5	issues 6:7,24 30:9,19	28:25 29:9 31:14	lessons 12:1
hyphenation 39:21	21:1,21 22:8 24:20	33:10,15 36:9 38:4	32:10,12 35:4	level 12:14
hypothetical 13:18	25:1,14,17 28:9		36:20 37:21	leveraged 17:22
14:3	29:25 31:17 35:1	J	knowing 36:15	Limewire 15:15,17
	35:25 36:13	J 39:25	knowingly 30:14	15:19,20 16:6,8,10
I	initial 2:12 38:23	jeopardy 38:7	knowledge 29:21	16:12,18,23 26:15
identifiable 24:20	injury 6:8,12 11:12	Jersey 3:11	33:20 39:9	26:15 30:24 31:4,6
25:14	11:13 20:10	job 12:15 31:1	known 11:22 14:14	31:9,19 32:4 33:20
identified 19:11	INOVA 24:18,22	jobs 14:19	16:19 17:4 19:20	34:17
identify 14:14 17:3	35:13	Johns 24:22 35:13	knows 4:25	limit 5:18,20 8:6
17:6,24,25 18:1,9	inside 17:19	Johnson 26:19 28:4		12:13 14:17
18:24 19:10,13,14	install 12:17 14:7	judge 2:20 4:3,7,14	L	limited 7:2 22:18
19:20 25:15	installation 16:14	4:21,24 5:3,23 6:1	lab 22:21 23:2,10	link 18:11 19:3,4,4
identifying 11:19	installed 15:15	6:4,9,13,16 7:1 8:3	24:19	listed 5:4
12:24 17:8 25:16	installing 13:25 14:9	8:5,18 9:13 10:8	Labcorp 35:14	little 4:22 15:4
30:4	installs 31:7	10:17,21,23 16:23	LabMD 2:6 4:4,5	LLP 3:18
		18:4,11,15 19:16	7:24 8:11,21 9:8	log 27:7

long 7:25 36:20 37:3	MEHM 3:8	17:25 18:19	offset 11:14 20:10	party 5:7
look 9:16,18 11:3 31:12 32:4 37:12 37:14	mentioned 30:3 36:3	needs 6:10 12:14	okay 4:3,7,14 6:1,13 7:1 10:23 19:16 23:22 31:13 33:6 35:2 38:21	pass 14:11
looking 17:15,16,17 17:18,21 18:24	mentions 27:19	negotiations 9:19	Once 17:19	pathology 22:21
loss 13:5 14:3,8	method 9:21	Neither 20:15	ongoing 8:2	patient 24:1,20 25:23,23,25
lot 38:14	methodology 10:3	network 12:7,9,11 15:9,10,13 17:19 17:20 18:10 20:1,3 20:3,6 31:10	online 18:2	patients 27:18
lots 11:22	Michael 2:19 38:13	networks 11:2 18:1 28:8	open 9:2 18:12	pay 18:16
low 14:7	microphone 6:10,17	never 8:22 24:9 33:23	opening 17:18	peer-to-peer 15:8 15:10
lowest 12:14 20:22	microphones 6:17	new 3:11 9:2,12 11:2 13:4 16:3	operate 19:1	pen 17:13,16,24 19:19
M	middle 6:18	nontechnical 12:19	operates 19:6	penetration 17:12 19:10
maintaining 12:21	million 34:22,22	Norton 18:12	operating 14:23	Pennsylvania 3:19
maintains 9:8	mine 32:7 38:10	notes 39:7	opportunity 4:18	people 5:4,11 8:22 15:12 16:19 19:25 32:13
making 18:20 24:6 29:10 32:19	minutes 8:7,9	notice 5:3 20:16,25 37:19	order 4:3 5:14,15 7:7,8 20:16,20,25 21:8	Pepson 38:13
maladies 23:18	mission 38:3	notwithstanding 33:15	orders 5:5 21:1	percent 25:24
malicious 18:25	mistake 12:8	notified 27:21	organizational 38:5	perform 12:15
manage 25:11	mistakes 16:19	notwithstanding 33:15	organizations 21:24 21:24	person 22:17
management 13:6,7 13:17 33:21 34:5	misunderstood 22:13	number 6:3 9:6 10:1 14:13 25:16 30:4 30:18 32:13 39:2	outside 17:15	personal 8:24 9:8 14:15,25 17:5
manager 15:16,17 16:17 22:16 24:4 26:12 33:19	misused 9:2,4 16:3	numbers 8:16 13:19 14:5 15:25 16:1 27:17 35:12	outsider 12:8,10 20:2	personally 25:14
manager's 15:20	modifications 5:14		overfiling 34:4	picture 24:16
managing 26:14	moment 8:1	O	overview 1:4 8:6	pieces 10:2,2
MARGARET 3:7	money 26:14 30:16	O 4:1 39:1,1,1,18,18 39:18,18	P	pitched 28:21
market 23:2	monitor 5:23		P 4:1 39:1,18	Pittsburgh 27:4
materials 9:24 11:23	motion 5:1 7:14,15 37:1		p.m 2:14 38:23	place 12:10 16:18 32:17
matter 2:5 37:13	motions 4:25 7:7,9 7:18,19 35:22 36:4 36:6 37:10		P2P 15:11,14 18:5 18:10,17,24 19:25 26:15 30:24 31:11	plan 12:20
mean 25:4 34:21,22	move 6:5 20:3 35:20		package 20:5	plans 13:6
meant 24:9 33:23	moves 37:13		PAGE 1:4	point 7:25 18:7,8,8 18:16,18 20:15 28:22,25
measure 12:5,6	music 26:16		paid 26:9,19 28:1 30:16	policies 12:22 34:19
measures 8:24 11:8 11:19 12:10,19,24 13:2,10 14:24 15:3 15:6 16:21 17:3,9 19:19 20:8,21	N		painlessly 37:14	policy 16:1 33:22 34:16
mechanics 34:11	N 1:1 4:1 39:1,18		paragraph 14:13 15:14 17:5	position 21:14 29:24 30:21 31:15,17 34:8
mechanism 7:3	N.W 3:11,19	OALJ 5:10	part 10:25	positions 32:20
media 19:3	name 38:12	objections 36:11	particular 11:20 20:21 22:24 25:23	possession 36:13
medical 8:12,16 9:4 16:2,4	names 8:15 13:19 14:4 15:24 16:1 27:17	objective 18:16	particulars 24:15	possible 13:10,10 37:14
meet 38:22	national 8:19,20 11:24 21:25	obligated 5:16	parties 4:8 5:5 7:3 7:25	posted 32:6
MEGAN 3:6	near 5:19	obligation 36:8	partner 38:9	potential 10:6 13:5
	necessarily 18:15	obtained 27:22 30:15		
	need 4:25 5:7,21 6:9 7:3 12:15 16:9,10 19:13	obviously 14:8 23:16 29:3 30:9 34:10		
	needed 14:18 16:21	office 5:4,7,9,12 24:21		
		offices 23:7		
		Official 5:6		

13:12 14:2,8 22:7 practical 11:25 practice 4:25 11:5 11:10,16 20:8 21:19 38:10 practices 9:12 14:17 20:1,13,16 preaching 18:14 preliminary 7:22 prescribes 20:16 present 3:24 8:6 16:6 presenting 6:21 press 27:8,15,18 30:3 pretrial 2:12 38:23 pretty 22:16,16 27:4 prevent 11:8 14:24 15:6 29:7 32:16 prevented 16:13 primarily 23:3 26:16 primary 34:5 principals 28:20 principles 11:21,23 12:3 prior 12:18 privacy 3:10 16:5 private 22:1 probably 24:20 probe 17:14 problem 19:7 procedures 12:22 25:7 proceeding 28:24 process 10:6 13:2 22:4 33:14 product 20:19 production 38:14 profession 21:5 professional 14:7 21:3 professionals 11:16 11:21,25 13:7,21 17:8 19:12 Professor 26:19 28:4	program 13:18,20 15:1,15 17:11 18:5 18:9,10,23,24 19:5 19:5,12 26:15 programs 12:17 16:19 17:21,23 18:25 proof 29:6,11,12 proofread 39:20 proofs 26:13 27:21 33:19 proprietary 32:6 propriety 33:17 prostate 23:17 protect 9:15 15:3 22:8 Protection 3:10 protocols 21:5 prove 27:12 32:23 proven 27:14 provide 7:15 12:25 20:22 21:20 37:5 provided 9:25 provider 16:1 provides 9:11 providing 12:20 public 2:15 9:23 13:21 33:23 34:16 publicized 12:1 publicly 32:24 33:1 published 11:23 punctuation 39:21 purchase 13:4 purchased 16:24 purposes 25:6 pursue 7:25 put 7:8 12:4 18:19 23:15 27:8,14 28:9 31:3 35:12 puts 30:3 putting 5:24 18:21 38:6	questions 8:8 quickly 6:5 37:13 quite 35:22 quote 11:17	released 24:2 29:25 33:4 reliance 11:1 remedies 36:8 Reported 2:25 represented 37:25 representing 4:11 4:17 request 4:22 require 20:18 requires 17:9 respect 7:14 Respondent 3:16 4:15,17 6:2 7:23 27:22 responding 12:21 responses 20:19 responsibility 34:5 responsible 22:17 result 19:21 36:15 results 8:17 retains 20:24 revenues 34:23 right 20:24 22:14 25:2 27:14 29:5 33:8 37:5 38:17 RIPOSO 3:5 risk 13:6,16,22,23 16:6,9,11 risks 14:15,17 17:4 17:8 18:1 19:11,14 19:20,21 RMR-CRR-CLR 2:25 39:16 role 35:17 Rubinstein 1:6 3:17 4:6,16,16,23 5:2 6:3,14,19 8:4 22:15,21 23:8,11 23:14,21,23 24:3 24:17,25 25:4,11 25:15,22 26:5,22 26:24 27:3,13 28:3 28:12,18 29:9,12 29:20 30:1 33:9 34:9,25 35:5,10,15 36:2,7,24 37:2,9	37:17,23 38:18 rule 7:9 10:13,14,15 21:14 ruled 7:12,17 rulemaking 10:8,12 rules 5:17 7:1,15 10:9,12 21:13 22:10 RYAN 3:8
		R	S	
		R 4:1 39:1,1,1,1,18 39:18,18,18 raising 36:9,10 rapidly 20:20 reads 10:15 real 26:11 really 19:13 reasonable 8:23 11:7,20 12:25 14:24 15:2 20:7,22 21:2,20 22:3,7 reasonableness 9:22 10:4 13:9 21:21 22:3 reasonably 11:13 14:15 17:4 19:20 20:11 reasons 35:11 rebuttal 6:22 receivable 25:12 26:6 receive 5:8,11 received 9:7 Reed 3:17 4:16 reed.rubinstein@... 3:22 refer 21:12,12 regard 9:13 10:13 regarding 7:6,6 regulation 21:14 34:6 regulations 21:13 22:10 reign 12:11 related 17:13 23:16 23:18 relationship 29:2 35:19 relatively 13:15 release 27:8,15,19 30:3	S 4:1 safeguards 10:14 Sam 26:25 sample 22:25 25:21 samples 8:12 22:20 24:19 SANS 22:1 SARA 39:25 saw 31:22 32:23 33:2 saying 8:19 10:24 21:17,21 27:25 29:5 32:11 34:7 says 19:3 33:2 scale 13:22 scan 17:13 scanning 20:18 schedule 4:20 scheduling 5:14 7:6 7:8 scope 37:11 second 12:13 17:2 30:20 33:12 Secretary 5:7 Section 9:10,10 11:5 21:12,19 33:11,14 security 8:15,23 10:25 11:8,19 12:5 12:6,10,16,20,21 12:22 13:2,9,19 14:5,16 15:1,3,25 16:20 17:7 19:24 20:1,7,13,16,19,21 20:22 21:1,2,2,20 22:8 27:3,4,17 28:6,8	

<p>see 7:4 22:23,25 27:6,7 32:9 35:2 37:6 seen 29:21 32:8 select 15:18 send 5:9 23:2,20 sends 23:25 24:19 sense 12:25 21:22,23 30:17 sensitive 8:14 11:6 12:12 15:3,23 17:22 19:25 20:4 21:20 sent 25:18,21 SEPTEMBER 2:13 39:4 series 9:20 35:21 36:4,9,10 serve 38:11 service 5:6 Services 34:1 serving 38:16 SESSION 2:15 set 9:19 10:2 11:10 12:7 13:8 14:13 17:5 sets 11:20 settings 12:16 settlement 7:21,23 7:24 8:1 seven 5:24 share 15:11 26:16 shared 15:8,22 16:7 16:7,15 24:9,12 31:18,19,22,25 33:22,23 34:8 sharing 16:16 19:24 Sheer 1:5 3:4 4:10 4:11 5:23 6:6,11 7:22 8:11,20 9:17 10:11,19,22,24 16:25 18:8,14,20 19:18 21:17 22:13 30:21,23 31:3,13 31:17,23 32:3,10 32:25 33:5,7 38:19 38:20</p>	<p>Shohl 3:18 38:9 show 26:13 27:21 31:23 32:25 33:19 shows 31:4 side 5:4 8:5 significant 30:10,18 33:9 similar 13:3 simple 22:16 26:11 single 12:4 17:6 sir 24:17 28:3 29:20 site 5:10 Sloane 3:25 small 18:25 22:18 22:23 33:17 34:21 34:24 35:3,6 38:7 Social 8:15 13:19 14:5 15:25 27:17 software 18:17,17 somebody 24:18 32:9 sooner 4:22 sorry 6:11 22:13 35:10 sort 23:18 25:7 sorts 21:6 27:15 sources 11:23 21:23 space 4:4 speak 6:10 specialty 22:23 specific 20:16 speculate 23:15 spell 26:21 spelling 39:21 spread 29:8,8 spreadsheet 24:4,8 24:21,24 25:10,13 26:7 spreadsheets 24:25 27:16 staff 22:18 38:12 stand 6:9,17 standard 26:6 34:19 standardized 16:2 standards 11:24 21:25 33:16 38:8,8 standpoint 26:11</p>	<p>start 4:8,9 7:16,19 starts 37:8 statements 9:23 states 2:1 23:3 statute 21:15 36:20 steal 9:4 27:7 30:16 step 12:24 stitch 20:2 stole 27:22 stolen 24:12 28:23 30:15 31:5 36:16 36:17 stop 16:16 18:6,13 stopped 16:12 store 13:18 storing 11:6 stretching 7:4 strong 21:1 study 28:3,5 subject 31:16 33:25 substantial 11:12 20:9 substantive 7:15,18 32:19 suggestion 36:21 Suite 3:19 sum 19:23 summary 7:8,10,12 supposed 34:15 sure 22:9 24:6,14 25:15,24 27:24 surrounding 23:3 surveil 26:20 Susanne 2:25 39:16 system 7:3 systematically 11:16 15:2 systems 14:23</p> <hr/> <p style="text-align: center;">T</p> <hr/> <p>T 39:1,1,1,18,18 T-I-V 26:24 table 8:2 take 4:18 8:9,13,23 14:23 22:6,20,25 24:11 38:3 taken 20:21 27:19</p>	<p>31:5 39:8 takes 13:11 23:19 talk 7:7 15:4 talking 18:4 19:17 27:14 taxpayer 30:16 technical 6:7,12,24 16:20 technically 23:24 technology 11:24 22:1 31:12 tell 7:11 17:8 19:12 22:19 28:16 telling 18:19 27:11 32:22 ten 9:5 test 8:16 17:12,16 17:17,20,20 19:10 28:7 33:12 testimony 6:21,22 28:19 29:14 tests 8:12 17:13,24 19:19 23:12 thank 4:7,18,18 5:2 8:11 21:10 22:14 28:22 33:8 38:17 38:18 thanks 5:14 theft 6:25 9:5 16:4 thieves 8:24 9:9 thing 7:6 things 21:6 26:10 31:6,6 34:12 36:14 think 5:13,16 25:22 26:16 29:15 35:25 thinking 6:4 Third 12:19 thorough 26:2 thought 18:22 35:3 thousands 8:15,18 13:19 threats 17:7 19:15 20:19 three 6:23 36:4 time 4:22 5:13,18 8:5,9 10:9 13:21 26:18 28:22,25</p>	<p>29:16 33:5 38:3,3 38:10,11 times 34:21 tissue 8:12 22:25 24:19 TITLE 39:3 Tiversa 24:13 26:18 26:22 27:9,21,25 28:5,6,25 29:14,15 29:22 30:3 32:11 34:10,11 36:21,24 Tiversa's 35:17 today 32:19 36:12 37:17 told 17:23 29:6 tomorrow 5:15 tool 17:6,10,11 19:14 tools 17:9 18:2 19:13 track 7:4 24:5 tracking 26:8 Trade 2:2 3:3,9 39:9 train 14:16 training 12:20 transcript 39:6,7,20 transparency 38:2 treasure 8:21 treatment 16:2,5 23:5 tremendous 10:1 trial 5:19 27:12 triggered 24:11 trove 8:21 try 28:1 trying 32:20 37:15 turn 17:2 turned 28:21 two 5:4,8,11 6:23 15:4 31:6,6 36:4 types 10:20</p> <hr/> <p style="text-align: center;">U</p> <hr/> <p>unauthorized 10:7 13:12 14:24 15:6 understand 24:5,5 24:15 27:24 31:11</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

31:12 36:5,11	vulnerability 13:20	Z	610 3:19
understanding	13:22,25 14:1,4	0	7
16:25 26:2 35:7	17:13,17,18 20:18	1	8
unfair 11:4,11 20:8	vulnerable 12:5	1 13:23 33:14	8 1:5 33:14
21:19	W	10 13:22,23,23	801 3:19
UNITED 2:1	Wait 24:14	14:13 17:5 34:22	9
unquote 11:17	want 5:11 9:9 23:15	100 25:24	9/25/2013 39:12
unreasonable 14:10	31:14 32:14 35:12	101 14:12	9300 15:24 19:25
update 13:25 14:7,9	36:19	12 29:16	9357 2:6 4:4 39:2
14:22	wanted 29:6	13-month 29:16	
upper 33:21	Washington 3:12,20	15 8:7,9 11:10 35:9	
USC 11:10	watchdog 38:1	18 15:14	
use 6:10,11,16,17	watching 5:23	180 32:21	
8:24 11:1,7 12:19	way 10:15,16 14:12	2	
15:2,5 16:19 17:3	20:3 22:4 26:6,8	2:00 2:14	
18:17 19:19	28:23 36:17	2:46 38:23	
user 12:14	ways 8:25 14:13	20,000 27:18	
user's 12:13	we're 5:18,20 18:20	20001 3:12	
users 12:15 14:21	19:7,9 21:17 29:3	20004 3:20	
15:11,17,19 16:8	29:16 30:1 35:21	2012 9:7	
uses 13:18	36:9,10 37:9,10	2013 2:13 39:4	
usually 17:8,12	Web 5:10	202 3:13,21	
utilize 9:15	weeks 36:4	210 7:2	
V	welcome 4:21	22 1:6	
VANCE 39:25	went 19:24 30:6	25 2:13 39:4	
VanDruff 3:5 4:12	white 23:10	3	
4:13	witness 31:21 32:23	326-2999 3:13	
variety 8:25 17:9	33:1	369,000 9:7	
19:13	witnesses 5:20,25	372-9100 3:21	
various 21:13 35:11	6:22 33:4 37:22	4	
verify 14:21	word 4:5,6	45(n) 11:10	
victim 28:15	work 23:1,6 24:7	5	
Victor 26:24	30:25 38:2	5 9:10,10 11:5 21:12	
Victoria 3:25	working 37:12	21:19 33:12 34:22	
view 31:3	works 6:19,19 10:16	5-0 35:9	
viewed 32:2	31:11	50 35:6,9,10	
violate 36:21	written 12:22	50/50 37:21	
violated 21:15 22:11	X	501(C)(3) 37:25	
violation 11:5	X 1:1	57 9:19	
virtue 31:18	Y	6	
virus 19:5	Yeah 28:7	601 3:11	
viruses 17:25 18:25	year 13:21		
voluntarily 31:18	years 9:5 11:22 18:3		
voted 7:13	32:6		
vulnerabilities 9:20			
17:21 20:2			