IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

MICHAEL J. DAUGHERTY
425 Broadland Rd., NW
Atlanta GA 30342

and

LABMD, INC.
425 Broadland Rd., NW
Atlanta GA 30342

Plaintiffs,

v.

ALAIN H. SHEER
(in his individual capacity)
4217 Sundown Rd.
Gaithersburg, Maryland 20882

and

RUTH T. YODAIKEN
(in her individual capacity)
4508 Chestnut St.
Bethesda, MD 20814

and

CARL H. SETTLEMYER, III
(in his individual capacity)
4805 20th St.
Arlington, VA 22207

and

DOES 1-10
(in their individual capacities),

Defendants.

Civil Action No. _____

JURY TRIAL DEMANDED

COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Michael J. Daugherty ("Daugherty") and LabMD, Inc. ("LabMD") (collectively, Daugherty and LabMD are referred to as "Plaintiffs"), by and through counsel, bring this action against Defendants Alain H. Sheer ("Sheer") in his individual capacity; Ruth T. Yodaiken ("Yodaiken") in her individual capacity; Carl H. Settlemyer, III ("Settlemyer") in his individual capacity; and Does 1-10, in their individual capacities (collectively, Sheer, Yodaiken, Settlemyer and Does 1-10 are referred to as "Federal Defendants"), and allege the following:

NATURE OF THE CASE

1. This *Bivens* action is based on an FTC investigation and prosecution fought so aggressively, abusively, unethically and illegally by FTC attorneys Sheer, Yodaiken and Settlemyer that they put a small cancer-detection firm in Atlanta, Georgia out of business. They did so without *any* incriminating evidence and by withholding exculpatory evidence not only from the targets of their investigation but also from responsible members of the FTC staff and FTC Commissioners who, based on the defendants lies and omissions, granted them authority to proceed with their illegal and unconstitutional pursuits. Every step of the way, the defendant FTC attorneys supported their actions with lies, thievery and testimony from a private company, Tiversa, whose business model was based on convincing companies to pay them to "recover" files that, in truth, *they* hacked from computers all over the world. The defendant FTC attorneys here knew or should have known from the very start of their investigation that their evidence and their arguments about unfair practices and impending consumer harm were fictional. These defendants gathered and relied upon stolen property, perjured testimony, documents from a sham organization and a company now known for stealing documents and lying about there whereabouts, all in the alleged interest of protecting consumers from unfair practices.

PARTIES

2. Daugherty, a resident and citizen of the state of Georgia, is over 18 years of age.

3. LabMD is a corporation organized and existing under the laws of the state of Georgia. Its principal place of business is located in Fulton County, Georgia. Daugherty is the sole owner of LabMD and is its president and chief executive officer.

4. Sheer is a resident and citizen of the state of Maryland, is over 18 years of age and can be served with process at 4217 Sundown Rd., Gaithersburg, Maryland 20882, or wherever he may be found. At all times relevant to this Complaint, Sheer has been an attorney employed by the Federal Trade Commission (the "FTC").

5. Yodaiken is a resident and citizen of the state of Maryland, is over 18 years of age and can be served with process at 4508 Chestnut St., Bethesda, MD 20814, or wherever she may be found. At all times relevant to this Complaint, Yodaiken has been an attorney employed by the FTC.

6. Settlemyer is a resident and citizen of the state of Virginia, is over 18 years of age and can be served with process at 4805 20th St., Arlington, VA 22207, or wherever he may be found. At all times relevant to this Complaint, Settlemyer has been an attorney employed by the FTC.

JURISDICTION AND VENUE

7. This Court has jurisdiction under 28 U.S.C. § 1331 and 28 U.S.C. § 1343. This case arises under the Constitution and laws of the United States of America. Daugherty and LabMD bring this action for damages against Federal Defendants named in their individual capacities, under *Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics*, 403 U.S. 388 (1971).

8. This Court has personal jurisdiction over the Federal Defendants because a substantial portion of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

9. Venue is proper in this District and this Division pursuant to 28 U.S.C. § 1391.

FACTUAL BACKGROUND

10. From at least 2001 through approximately January 2014, LabMD operated as a small, medical services company providing doctors with cancer-detection services.

11. In connection with its testing and other services, LabMD collected and maintained certain personal information on thousands of patients ("Personal Information"). For purposes of this Complaint, Personal Information means "individually identifiable information from or about an individual consumer including, but not limited to: (a) first and last name; (b) telephone number; (c) a home or other physical address, including street name and name of city or town; (d) date of birth; (e) Social Security number; (f) medical record number; (g) bank routing, account, and check numbers; (h) credit or debit card information, such as account number; (i) laboratory test result, medical test code, or diagnosis, or clinical history; (j) health insurance company name and policy number; or (k) a persistent identifier, such as a customer number held in a "cookie" or processor serial number." Personally Identifiable Information ("PII") is a subset of the data in Personal Information, including a person's name, address, date of birth, Social Security number, credit card and banking information, and drivers' license number.

12. Personal Information collected and maintained by LabMD includes information protected by privacy requirements set forth in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). LabMD has at all times complied with HIPAA.

13. Various state and federal laws prohibit the unauthorized taking, possession and disclosure of PII and Personal Information. *See, e.g.,* 42 U.S.C. § 1320d-6(a)(2) (criminal violations for obtaining individually identifiable health information relating to an individual and/or disclosing individually identifiable health information to another person);

14. Various state and federal laws prohibit hacking of computers to obtain information and documentation, including PII and Personal Information. *See, e.g.,* O.C.G.A. §16-9- 93 (criminal violations for computer theft, computer trespass, computer invasion of privacy, or computer forgery).

15. Tiversa Holding Corp. ("Tiversa") is a privately held company headquartered in Pittsburgh, Pennsylvania. Tiversa was founded by Robert Boback ("Boback") and Samuel Hopkins ("Hopkins") in January 2004.

16. Hopkins, a high-school dropout, left Tiversa in 2011.

17. Prior to joining Tiversa, Boback was a practicing chiropractor who dabbled in various activities such as buying and selling residential properties and selling cars on eBay.

18. At all times relevant to this Complaint, Boback has been the chief executive officer of Tiversa.

Tiversa

19. Tiversa is a data security company that offers breach detection and remediation services. Tiversa uses a combination of off-the-shelf and proprietary technology purportedly to search entire peer-to-peer networks for documents of interest to its customers or potential customers and downloads the documents it finds into its data storage devices. Tiversa has claimed that it "provides P2P intelligence services to corporations, government agencies and

individuals based on patented technologies that can monitor over 550 million users issuing 1.8 billion searches a day."

20. Tiversa searches for and downloads data from peer-to-peer networks. The data is kept in what is referred to as Tiversa's "data store" ("Data Store"). The Data Store contains files that Tiversa has downloaded from peer-to-peer networks. The Data Store also contains information as to where the downloaded files had been located.

21. Tiversa does not seek permission to access computers or download files from computer workstations, even though it knows that much of what it finds and downloads to its Data Store are files that were never intended to be shared.

22. Tiversa's business model is to capitalize on finding and downloading files that were never intended to be shared. Thus, Tiversa is particularly interested in finding and downloading items such as individual and corporate tax returns, medical records, social security numbers, credit card numbers, passwords, employment records, trade secrets, privileged and protected information, military and other state secrets, PII and Personal Information. Tiversa collects such files without permission or authority, even though there are state and federal laws designed to prevent this kind of information gathering and storage.

23. Tiversa purports to be a white knight in the world of inadvertent file sharing.

24. The amount of inadvertently shared files searched for, located and stored by Tiversa is massive.

25. Boback has testified to Congress that Tiversa downloads "the equivalent of the Library of Congress every three days."

26. Tiversa claims to be able to see entire peer-to-peer networks, instead of a smaller subset as seen by an individual user.

27. There are two ways for data to get into Tiversa's Data Store: (1) Tiversa's proprietary program, Eagle Vision, automatically downloads files returned from Tiversa's automated searches and (2) Tiversa's forensic analysts insert data that the analysts find using a stand-alone computer running a peer-to-peer client (*e.g.*, LimeWire).

28. In Tiversa's searches for exposed files on peer-to-peer networks, Tiversa records in its Data Store (1) the information disclosed, (2) the IP address of the disclosing computer, (3) metadata from the file, (4) the identity of the disclosing company and (5) when the information was disclosed. Much of this information is included on spreadsheets that Tiversa analysts update several times a day. The purpose of the spreadsheets is so that Boback and the Tiversa sales force can make sales calls to the affected companies.

29. When contacting the affected company to sell services, Tiversa's practice was to not reveal the source of the information and to tell the potential customer that Tiversa had not recorded the IP information. Tiversa would provide the found documents to the potential customer only after stripping the IP address and removing any metadata relating to the disclosure source, while keeping a separate set of the files that included disclosure source information.

30. Tiversa monetizes information it obtains from peer-to-peer networks either by selling a monitoring contract (pursuant to which Tiversa would search for certain key words for a period of time), or by selling a "one-off" service (which would remediate just the existing disclosure problem). Tiversa typically creates an "incident response" for its "one-off" services.

31. Tiversa often fabricates information and documentation regarding the disclosing source of files it finds on peer-to-peer networks. If a potential customer would not purchase Tiversa's services, Tiversa would often attempt to monetize peer-to-peer network findings by

notifying an *existing* Tiversa customer of the source of the customer's information and advising the *existing* customer to contact Tiversa's target.

32. When a company refused to purchase Tiversa's services, Boback would often tell his analysts, in reference to that company, to the effect of, "you think you have a problem now, you just wait." In many of these situations, Boback directed Tiversa analysts to input information into Tiversa's Data Store so as to make that company's information "proliferate" and thereby make it appear, fraudulently, that a file had "spread" to multiple places. Tiversa would then use this "evidence" to follow up with a company to try again to get the company to purchase Tiversa's remediation services.

33. For companies that initially refused to purchase Tiversa's services, Tiversa would often follow up with the target by stating, fraudulently, that the disclosed document had spread to additional IP addresses, including IP addresses of known "bad actors" or identity thieves. In such cases, Tiversa's analysts would alter or create source and spread information in the Data Store to make it appear that Tiversa had located and downloaded the file from the IP address of a known bad actor and that files had proliferated on peer-to-peer networks.

34. Starting as early as 2006, Tiversa created an Advisory Board whose members came to include General Wesley K. Clark (retired general of the United States Army; former candidate for President of the United States of America); Maynard Webb (former chief operating officer for eBay); Dr. Larry Ponemon (chairman and founder of the Ponemon Institute); Howard Schmidt (former Chief Security Strategist for the U.S. CERT Partners Program for the National Cyber Security Division, Department of Homeland Security and former Vice President and Chief Information Security Officer and Chief Security Strategist for eBay); Michael Dearing (former Senior Vice President & General Merchandise Manager for eBay); Thomas Keeven (former Vice

President of Infrastructure, Vice President of Operations and Vice President of Architecture for eBay); Lynn Reedy (former Chief Technical Officer and Senior Vice President of Product & Technology for eBay) and Patrick Gross (a founder and former chairman of the executive committee of American Management Systems, Inc.).

35. On July 24, 2007, Boback testified in a hearing before the U.S. House of Representatives Committee on Oversight and Government Reform (the "Oversight Committee") on the topic of inadvertent file sharing over peer-to-peer networks.

36. Tiversa Advisory Board member Wesley Clark also testified at that hearing, immediately after Boback. Among other statements, General Clark testified as follows:

> I want to just disclose now that I am an advisor to Tiversa, and in that role I do have a small equity stake in Tiversa. But my engagement here has just opened my eyes to activities that I think, if you saw the scope of the risk, I think you would agree that it is just totally unacceptable. The American people would be outraged if they were aware of what is inadvertently shared by Government agencies on P2P networks. They would demand solutions.
>
> As I was preparing for the testimony, I asked Mr. Boback to search for anything marked classified secret, or secret no-foreign. So he pulled up over 200 classified documents in a few hours running his search engine. These documents were everything from in sums of what is going on in Iraq to contractor data on radio frequency information to defeat improvised explosive devices. This material was all secret, it was all legitimate.
>
> Even more alarming, I got a call from Bob Boback on Wednesday night that he had found on the peer-to-peer net the entire Pentagon's secret backbone network infrastructure diagram, including the server and IP addresses, with password transcripts for Pentagon's secret network servers, the Department of Defense employees' contact information, secure sockets layer instructions, and certificates allowing access to the disclosing contractors' IT systems, and ironically, a letter from OMB which explicitly talks about the risks associated with P2P file-sharing networks. So I called the Office of the Secretary of Defense. I got the right people involved. They had some meetings on it this. It turns out that a woman with top-secret clearance working for a contractor on her home computer, she did have LimeWire, and somehow, I guess, she had taken some material home to work on it, and so all this was out there.
>
> But these two examples illustrate the risks that are out there. Peer-to-peer file sharing is a wonderful tool. It is going to be a continuing part of the economy. It is a way that successfully moves large volumes of data, and that is not going to go away, but it has to

> be regulated and people have to be warned about the risks, and especially our Government agencies - our National Security Agency, DOD, people that run the Sipranet - have to take the appropriate precautions, because we can't have this kind of information bleeding out over the peer-to-peer network.

37. Boback and General Clark's testimonies caught members of Congress and several federal agencies off guard. Tiversa, Boback and General Clark appeared to have more insight, more actual examples, more evidence, more technological capabilities, more expertise and more awareness of the problems of inadvertent file sharing on peer-to-peer networks than those in the federal government who believed this issue was their responsibility, including the Federal Trade Commission.

Tiversa and the FTC Agree to Cooperate

38. Boback, Settlemyer and other FTC staff members began communicating approximately two months after the 2007 Congressional hearing on inadvertent file sharing. These communications were as frequent as weekly during some periods. The subject matter of these communications was information available on peer-to-peer networks.

39. Boback believed he could capitalize on Tiversa's newfound arrangement with the FTC by reporting to the FTC companies that refused Tiversa's services, the expected result of which was that those companies would respond to FTC inquiries by hiring Tiversa.

40. The FTC intended to capitalize on its relationship with Tiversa by using Tiversa's technological capabilities and expertise to identify targets for investigations and prosecutions and by using evidence obtained from Tiversa to prosecute.

41. In the fall of 2007 or winter of 2007/2008, members of the FTC staff visited Boback at Tiversa's facility in Pennsylvania. Following that meeting, the FTC began requesting that Tiversa provide information to the FTC. Tiversa, Settlemyer and other members of the FTC

staff essentially agreed that, in the world of cybersecurity, Tiversa would be the FTC's stalking horse.

Peer-to Peer Networks

42. In peer-to-peer networks, computer files (*e.g.,* music, videos and pictures) can be shared directly between computers connected to one another via the internet.

43. Peer-to-peer file-sharing applications (*e.g*., LimeWire) enable one computer user to make a request to search for all files that have been made available for sharing by another computer user, so long as the other computer is also using the file-sharing application.

44. Users of peer-to-peer networks perform searches using terms related to the particular file they hope to find and receive a list of possible matches. The user then chooses a file they want to download from the list.

45. The search capabilities on peer-to-peer networks are limited. For example, peer-to-peer networks are only capable of searching for filenames. These networks do not have the capability for users to search for files using words or other data contained *in* the files that have been made available for sharing by other users. In addition, search terms must be precise. With LimeWire, for example, a user searching for files with the search terms "insurance" and "aging" would not find any insurance aging files with the filename "insuranceaging."

46. A document being "shared" or "made available for sharing" on a peer-to-peer network is available to be downloaded by another computer user on the same peer-to-peer network. The fact that a document is being shared, or made available for sharing does not mean the document has been "downloaded" for viewing or is immediately viewable. The contents of a file that is available for sharing are not disclosed until the file is downloaded and viewed by the requesting user.

47. In many cases, files that are "shared" on a peer-to-peer network are shared without the knowledge of the user of a computer that has a file sharing application on it. The user may not even know that the computer he or she is using has a file sharing application. Such situations are often referred to as "inadvertent file sharing via P2P networks." Considerable research has been done and papers written on the topic. *See, e.g.,* "Filesharing Programs and "Technological Features to Induce Users to Share,"" A Report to the United States Patent and Trademark Office from the Office of International Relations, Prepared by Thomas D. Sydnor II, John Knight and Lee A. Hollaar (November 2006).

Tiversa's Theft of LabMD's Property

48. In May 2008, Tiversa targeted LabMD as a potential customer. Tiversa contacted LabMD to inform it that a LabMD file containing Personal Information was available through LimeWire. This particular file was a 1,718-page PDF document containing Personal Information on approximately 9,300 patients (the "1718 File"). The 1718 File was victim of inadvertent file sharing.

49. In truth, Tiversa had, without any authority, accessed and downloaded ("hacked") the 1718 File from a LabMD billing computer in Atlanta, Georgia on February 25, 2008. Tiversa's unauthorized download and retention of Personal Information was a violation of several state and federal crimes.

50. The filename on the document Tiversa hacked was "insuranceaging_6.05.071.pdf". The chance that anyone would ever have searched for or found the 1718 file was extremely remote. In order for Tiversa to receive a search result for the "insuranceaging_6.05.071.pdf" file, it would have to have searched for the document using the highly unusual search terms "insuranceaging" or "6.05.071".

51. Only Tiversa, with its "patented technologies that can monitor over 550 million users issuing 1.8 billion searches a day" and its cadre of highly experienced professional hackers, would ever have found the 1718 File.

Tiversa's Lies to LabMD

52. Immediately after Tiversa's call, LabMD investigated and determined that the 1718 File was inadvertently available because, unbeknownst to LabMD, LimeWire was installed on a LabMD billing computer. LabMD determined within minutes that LimeWire was installed on only one of its computers and removed the LimeWire application right away.

53. As part of LabMD's investigation regarding the 1718 File, LabMD employees constantly searched peer-to-peer networks for the 1718 File until 2013. Those employees were never able to find the 1718 file on any peer-to-peer network.

54. Soon after Tiversa first contacted LabMD in May 2008, it began a series of efforts to convince LabMD to purchase its remediation services. These efforts continued from mid-May through mid-July 2008.

55. During these sales efforts, Tiversa told LabMD that its patented technology and forensic experts had determined that the 1718 File was being searched for on peer-to-peer networks and that the 1718 File had spread across peer-to-peer networks. Except to the extent Tiversa observed LabMD employees searching for the 1718 file, these were lies.

56. On May 13, 2008, a Tiversa analyst specifically told LabMD the following:

- "our system shows a record of continued availability for sporadic periods over the past several months but we did not attempt to download it again."
- "The system did not auto-record the IP, unfortunately, most likely due to the little amount of criteria indexed against the DSP. "

- "The actual source IP address in the data store logs [is] not readily available at this point. If it is there, I should be able to get it but it would take some time."

These were lies.

57. On May 22, 2008, Tiversa told LabMD, "We have continued to see people searching for the file in question on the P2P network by searching precisely for the exact file name of the file in question. They may or may not have been successful in downloading the file however." Except to the extent Tiversa observed LabMD employees searching for the 1718 file, these were lies.

58. On July 15, 2008, Tiversa told LabMD that it "continued to see individuals searching for and downloading copies of the [1718 File]." This was a lie. No one was downloading copies of the 1718 File because it was not available for sharing on any peer-to-peer network.

59. On July 22, 2008, LabMD instructed Tiversa to direct any further communications to LabMD's lawyer.

60. Tiversa's sales tactics became even more aggressive. On November 21, 2008, Jim Cook, one of Tiversa's attorneys, told an attorney for LabMD that he had been talking to the FTC about LabMD. Cook justified his actions by claiming that Tiversa was concerned about being sued for having knowledge of the "breach" and not reporting it as required by law. This was a lie. Tiversa had no such concern.

61. When Boback learned that Mike Daugherty at LabMD ultimately refused to do business with Tiversa, Boback said to one of Tiversa's analysts, "f--- him, make sure he's at the top of the list." The "list" was a spreadsheet of companies Tiversa would soon give to the FTC.

Tiversa's Lies to CIGNA

62. One of the insurance companies listed in the 1718 file was CIGNA Health Insurance ("CIGNA"). In 2008, CIGNA was a Tiversa customer.

63. In April 2008, Tiversa sent an incident report to CIGNA stating that it had found a file on a peer-to-peer network with Personal Information on CIGNA insureds. Tiversa stated, "[a]fter reviewing the IP address resolution results, meta-data and other files, Tiversa believes it is likely that LabMD near Atlanta, Georgia is the disclosing source." This was *not* a lie.

64. In a report dated August 12, 2008, however, Tiversa told CIGNA, "The [1718 File], as well as some of the files not related to CIGNA, have been observed by Tiversa at additional IP addresses on the P2P." This was a lie.

65. Tiversa also told CIGNA in the August 12, 2008 report that (1) it had found the 1718 File in San Diego, CA at IP address 68.8.250.203 (designated "Proliferation Point #2") and (2) "other files present at Proliferation Point #2 suggest that this source could be an Information Concentrator." These were lies.

The FTC Strengthens its Alliance with Tiversa

66. Communications between Tiversa and the FTC continued through the winter and spring of 2009. Settlemyer introduced Sheer to Boback on or about March 4, 2009.

67. On information and belief, Settlemyer or Sheer (or both) introduced Yodaiken to Boback and others at Tiversa in the spring of 2009.

68. Sheer, Yodaiken and Settlemyer knew about the 1718 File in the spring of 2009.

69. Sheer, Yodaiken and Settlemyer knew or should have learned in the spring of 2009 that the filename of the 1718 file was "insuranceaging_6.05.071.pdf".

70. Sheer, Yodaiken and Settlemyer learned or should have learned in the spring of 2009 that the disclosing source of the 1718 File was an IP address for LabMD in Atlanta, Georgia.

71. Sheer, Yodaiken and Settlemyer learned or should have learned in the spring of 2009 that the *only* source of the 1718 File was an IP address for LabMD in Atlanta, Georgia.

72. Sheer, Yodaiken and Settlemyer learned or should have learned in the spring of 2009 that the 1718 File had not proliferated or spread anywhere on any peer-to-peer network.

The List

73. By the spring of 2009, Tiversa had developed a spreadsheet of approximately 100 companies that, according to Tiversa, had exposed Personal Information (the "List"). The companies on the List were companies to which Tiversa had tried but failed to sell Tiversa's remediation services. Tiversa scrubbed the List of the names of all existing or prospective Tiversa customers. As dictated by Boback, LabMD was included and placed near the top of the List.

74. Tiversa would later claim that it included several of its own customers on the List. This was a lie.

FTC Procedures and Rules of Practice

75. The behavior of FTC employees is mandated by the FTC's Procedures and Rules of Practice ("PRP") – the official rules of the agency.

76. "Commission investigations" under the PRP are inquiries conducted by a "Commission investigator" for the purpose of ascertaining whether any person is or has been engaged in any unfair or deceptive acts or practices in or affecting commerce or in any antitrust violations.

77. Under the PRP, the term "Commission investigator" means any attorney or investigator employed by the Commission who is charged with the duty of enforcing or carrying into effect any provisions relating to unfair or deceptive acts or practices in or affecting commerce or any provisions relating to antitrust violations.

78. At all times relevant to this Complaint, Defendants Sheer, Yodaiken and Settlemyer were Commission investigators.

79. The PRP authorizes the FTC to utilize civil investigative demands ("CIDs") in certain limited circumstances. The FTC does not have the authority to issue CIDs in the absence of an investigation.

80. The PRP mandates that each CID shall state the nature of the conduct constituting the alleged violation that is under investigation and the provision of law applicable to such violation.

81. Under the PRP, the production of documentary material in response to CIDs "shall be made under a sworn certificate, in such form as the demand designates, by the person, if a natural person, to whom the demand is directed or, if not a natural person, by any person having knowledge of the facts and circumstances relating to such production, to the effect that all of the documentary material required by the demand and in the possession, custody, or control of the person to whom the demand is directed has been produced and made available to the custodian."

The Privacy Institute

82. In the spring and summer of 2009, Sheer, Yodaiken and Settlemyer came to learn or should have come to learn that Boback and others at Tiversa were not honest or trustworthy. Sheer, Yodaiken and Settlemyer knew or had reason to know that Tiversa's internal documents

would prove that Boback and others at Tiversa could not be trusted and further knew or had reason to know that Tiversa's internal documents were likely to disprove allegations Tiversa would make about the source and spread of documents it "found" on peer-to-peer networks. Sheer, Yodaiken and Settlemyer also knew or had reason to know that Tiversa analysts would alter information in the Data Store to make it appear that Tiversa had located and downloaded files from the IP addresses of known identity thieves and further knew or had reason to believe that Tiversa analysts would create information in the Data Store as evidence of spread where, in fact, no spread had ever occurred.

83. Sheer, Yodaiken and Settlemyer knew or had reason to know that it would be extremely difficult, if not impossible, for companies the FTC investigated and prosecuted to disprove Tiversa's "evidence" of source and spread, unless those companies had access to Tiversa's internal documents.

84. Neither Sheer, Yodaiken, Settlemyer nor Boback wanted Tiversa to produce to the FTC any internal documents that would disprove Tiversa's evidence of source and spread. Specifically, Sheer, Yodaiken, Settlemyer and Boback did not want the FTC to use a compulsory process to obligate Tiversa to produce anything. To keep Tiversa from being legally obligated to produce *any* documents and to give Boback and Tiversa the freedom to produce whatever they wanted to the FTC, Sheer, Yodaiken, Settlemyer, Boback and others at Tiversa agreed that (1) Boback and Tiversa would create a shell company, (2) the FTC would issue a CID to the shell company instead of Tiversa, (3) Boback and Tiversa would "give" the shell company documents of their choosing, including a limited number of documents that supposedly contained incriminating evidence on future targets of FTC investigations and enforcement actions and (4) Boback and Tiversa could withhold from production whatever they wanted.

85. The shell company, created on June 3, 2009, was named "The Privacy Institute."

86. The Privacy Institute had no assets or employees. It was not legally related to Tiversa. Tiversa had no legal obligation to provide anything to The Privacy Institute and The Privacy Institute had no legal requirement to obtain anything from Tiversa.

87. By law, Sheer, Yodaiken and Settlemyer needed an FTC Commissioner to approve and sign the CID that would be served on The Privacy Institute on or about July 10, 2009.

88. By law, the CID could only issue in connection with an FTC investigation.

89. Tiversa was never the target of an FTC investigation or enforcement action.

90. The Privacy Institute was never the target of an FTC investigation or enforcement action.

91. Sheer and Yodaiken knew that the FTC was not authorized to issue CIDs with nothing more than a blanket request and knew that no FTC Commissioner was likely to sign such a CID. To induce an FTC Commissioner to sign and authorize a CID to be served on The Privacy Institute (the "PI CID"), Sheer and Yodaiken included in the proposed PI CID requests related to two companies already under investigation by the FTC – Rite-Aid and Walgreens. Sheer and Yodaiken also included a blanket request written to capture information on companies like LabMD that were *not* under investigation by the FTC. Sheer and Yodaiken knew this was improper, if not illegal, and knew that The Privacy Institute was just a façade. Sheer and Yodaiken were not concerned about the consequences of these actions because they knew that neither Tiversa nor The Privacy Institute would ever complain.

92. The FTC Commissioner who authorized and signed the PI CID would not have done so had he been told that Sheer and Yodaiken had plans to investigate parties other than

Rite-Aid and Walgreens that, like LabMD, had (1) already resolved any disclosure issues, (2) de minimus disclosures, (3) no disclosures, (4) no complaining witness, and (5) no originating source other than the company that would become the target of Sheer and Yodaiken's investigations.

93. Sheer, Yodaiken and Settlemyer knew that The Privacy Institute had no assets, no employees, no physical location and no documents or files. The Federal Defendants nevertheless served the PI CID on The Privacy Institute on or about July 10, 2009. Because The Privacy Institute had no documents, files or employees, the PI CID had no force of law. As a result, neither Tiversa nor The Privacy Institute had any obligation to produce *anything* to the FTC. Instead, Tiversa was free to provide whatever it wanted to the FTC.

94. In the fall of 2009, Boback and a Tiversa forensic analyst name Richard E. Wallace met in Washington, D.C. with Sheer, Yodaiken and/or other members of the FTC staff to discuss Tiversa's response to the CID served on The Privacy Institute. On information and belief, the FTC Staff expressed concerns that it did not have enough evidence to investigate companies where the only disclosing source was the company the FTC wanted to pursue.

95. On the return trip from Boback and Wallace's meeting with the FTC, Boback told Wallace that Tiversa needed to increase the apparent "spread" of the files identified on the List. Wallace was to search for the files again to see if they were available at IP addresses in addition to the address in the Data Store, and that if the files were not, in fact, available at any additional IP addresses, Wallace was told to create or alter data in the Data Store to make it appear that the files were available at additional IP addresses.

96. On information and belief, Sheer, Yodaiken, Settlemyer and Boback expressly or tacitly agreed and conspired in 2009 that Boback and Tiversa would provide whatever evidence

the FTC needed in its investigation and enforcement of companies on the List, even if the evidence was fraudulent. In so doing, Sheer, Yodaiken and Settlemyer conspired to deprive LabMD and Daugherty of their constitutional rights. LabMD and Daugherty were deprived of their constitutional rights as a result of this conspiracy.

97. On information and belief, Sheer, Yodaiken, Settlemyer and Boback expressly or tacitly agreed and conspired in 2009 that Boback and Tiversa would provide the FTC false evidence of source and spread. In so doing, Sheer, Yodaiken and Settlemyer conspired to deprive LabMD and Daugherty of their constitutional rights. LabMD and Daugherty were deprived of their constitutional rights as a result of this conspiracy.

98. On information and belief, Sheer, Yodaiken and Settlemyer knew or should have known in 2009 and thereafter that Boback and Tiversa would, upon request for additional evidence, manufacture and provide false evidence of source and spread. Sheer, Yodaiken and Settlemyer expressly or implicitly conspired to allow this to happen and thereby deprived LabMD and Daugherty of their constitutional rights.

99. On information and belief, Sheer, Yodaiken and Settlemyer knew or should have known in 2009 and thereafter that Boback and others at Tiversa had and would provide false sworn testimony concerning source and spread. Sheer, Yodaiken and Settlemyer expressly or implicitly conspired to allow this to happen and thereby deprived LabMD and Daugherty of their constitutional rights.

100. On information and belief, Sheer, Yodaiken, Settlemyer and Boback expressly or tacitly agreed and conspired in 2009 that Boback and Tiversa would withhold from production to the FTC and third parties documents and things that were exculpatory to LabMD and Daugherty.

Sheer, Yodaiken and Settlemyer expressly or implicitly conspired to allow this to happen and thereby deprived LabMD and Daugherty of their constitutional rights.

101. On information and belief, Sheer, Yodaiken, Settlemyer, Boback and Tiversa expressly or tacitly agreed and conspired in 2009 to hurt, if not destroy, LabMD and to deprive Daugherty of his livelihood and property. Sheer, Yodaiken and Settlemyer expressly or implicitly conspired to make this happen and thereby deprived LabMD and Daugherty of their constitutional rights.

102. Boback wanted revenge. Sheer, Yodaiken and Settlemyer wanted to make an example of LabMD. They believed, or should have known, that LabMD did not have the resources to sustain the kind of investigation they had in store for LabMD and Daugherty.

103. On July 27, 2009, Boback testified to the Oversight Committee on the topic of inadvertent file sharing for a second time. Boback testified that in February of that year, "Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One [the President's helicopter]. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran." This was a lie. Tiversa never found any files relating to Marine One on a computer with an IP address in Iran. On information and belief, Sheer, Yodaiken and Settlemyer knew this was a lie yet failed and refused to disclose their knowledge to responsible individuals at the FTC or other law enforcement agencies.

104. In August 2009, Tiversa, under the guise of The Privacy Institute, gave the List to the FTC. Tiversa also produced a screen shot showing that the disclosing source for the 1718 File was a computer with an IP address for LabMD in Atlanta, GA. Daugherty and LabMD would not know about this document or Sheer and Yodaiken's knowledge of it until years later.

Sheer and Yodaiken should have but refused to produce this document to Daugherty or LabMD at anytime during their investigation of Daugherty and LabMD.

105. Neither Tiversa nor The Privacy Institute ever provided any evidence that the 1718 File had proliferated on a peer-to-peer network. Sheer, Yodaiken and Settlemyer knew this but, on information and belief, consciously disregarded and failed to disclose these facts to responsible individuals at the FTC.

106. Daugherty and LabMD would not learn anything about The Privacy Institute before Boback's deposition on November 21, 2013. Until that point in time, neither Daugherty nor LabMD knew or had reason to know that Sheer, Yodaiken and Settlemyer, in their individual capacities:

- were acting outside the scope of their employment;
- were acting *ultra vires*;
- had deceived their superiors and others at the Commission;
- knew that Boback and Tiversa had committed crimes;
- were conspiring with Boback and Tiversa to create fraudulent incriminating evidence against LabMD and Daugherty;
- were conspiring with Boback and Tiversa to withhold evidence exculpatory to LabMD and Daugherty;
- were withholding evidence exculpatory to them; and
- were explicitly or implicitly conspiring to deprive Plaintiffs of their constitutional rights.

The FTC Gives Confidential Information to Boback

107. At some point before October 6, 2009, Sheer and/or Yodaiken violated FTC rules, policies, procedures and/or FTC guidance by disclosing to Boback intimate details about the FTC's upcoming investigations of the 100 or so companies on the List.

108. In October 2009, Boback bragged to employees of LifeLock about having inside knowledge from the FTC. Specifically, Boback told LifeLock on October 26, "the FTC is preparing the federal cases against 100 or so companies that have breached consumers information via P2P." On October 6, Boback told LifeLock, "The FTC letters did not go out yet so the companies will not know what you will be talking about...yet."

109. Boback further explained to LifeLock that the Washington Post planned to "shame" companies into addressing the problem, and that the upcoming FTC investigations presented a unique opportunity for LifeLock and Tiversa to profit.

110. On October 20, 2009, a Tiversa analyst e-mailed Boback the name, resume, and Facebook profile picture of a House Ethics Committee staffer who would become part of a story published by the Washington Post nine (9) days later. Boback thereafter told LifeLock "…there was a breach in House Ethics via 2P2 that the Washington Post will be writing a story about this week or next…." Boback knew this because Boback gave the information to the Washington Post.

111. On information and belief, Boback bragged to Sheer, Yodaiken and Settlemyer about he and Tiversa being the undisclosed sources for the Washington Post story.

112. Boback thereafter tried to get the House Ethics Committee to hire Tiversa by showing the "spread" on the leak.

113. From August 2009 through January 2010, Tiversa employees called Defendant Sheer at least 34 times.

114. On December 22, 2009, the White House announced that President Obama appointed Howard Schmidt to be the President's new White House Cybersecurity Coordinator. On information and belief, Schmidt was still a member of Tiversa's Advisory Board at the time of his appointment. On information and belief, Schmidt had an equity interest in Tiversa at the time of his appointment. On information and belief, Schmidt kept his equity interest in Tiversa during his service as White House Cybersecurity Coordinator. On information and belief, at Boback's behest, Schmidt influenced the FTC in general and Sheer in particular, to vigorously pursue an investigation and enforcement action against LabMD, regardless of the merits of the pursuit. On information and belief, Sheer told or otherwise indicated to Schmidt that he would.

115. Soon after the announcement of Schmidt's appointment, Daugherty received a letter dated January 19, 2010, from Sheer informing LabMD that the FTC was "conducting a non-public inquiry into LabMD's compliance with federal law governing information security." The letter states, "According to information we have received, a computer file (or files) from your computer network is available to users on a peer-to-peer file sharing ("P2P") network (hereinafter, "P2P breach"). This was a lie. Sheer knew that neither the 1718 File nor any other LabMD file was available to anyone on any peer-to-peer network. On information and belief, Sheer knew from conversations with Boback and others that when Tiversa contacted LabMD in May 2008, LabMD immediately found and removed the offending software (LimeWire) and that, thereafter, there was no basis for an inquiry or investigation of any sort.

116. The FTC's investigation of LabMD and Daugherty (the "Investigation") continued for three and a half years. It was an intrusive and exhaustive, multiyear civil

investigation in which Sheer and Yodaiken issued burdensome voluntary access requests and civil investigative demands to LabMD, obtained thousands of pages of documents from LabMD and Daugherty, and deposed, under oath, LabMD principals, causing LabMD's insurance carriers to cancel LabMD's insurance coverage and causing crippling economic hardship and reputational harm.

117. LabMD and Daugherty produced thousands of pages of documents, sat for hours of interviews and met with the FTC on numerous occasions by telephone and in person, only to be told by Sheer and Yodaiken, time after time, that LabMD's responses were inadequate.

118. At no time during the Investigation did Sheer, Yodaiken or Settlemyer disclose to LabMD the evidence the FTC received from The Privacy Institute establishing that LabMD was the *only* source of the 1718 File. Nor did they disclose their knowledge that Tiversa obtained the 1718 file by hacking into LabMD's computer network.

119. At no time during the Investigation did Sheer, Yodaiken or Settlemyer inform LabMD that the FTC had received documents from Tiversa via The Privacy Institute, a sham organization.

120. At no time during the Investigation did Sheer or Yodaiken issue a CID to Tiversa for documents and information relating to the 1718 File.

121. Not a single patient has ever been harmed by the alleged disclosures of the 1718 file.

122. On August 31, 2011, the FTC demanded that Daugherty and LabMD sign consent decrees admitting to an unfair trade practice under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, due to inadequate data security practices. LabMD and Daugherty refused to

sign the consent decrees, making their positions clear to Sheer and Yodaiken on October 20, 2011.

123. In retaliation for Daugherty and LabMD's refusals to sign consent decrees, the FTC issued CIDs to LabMD and Daugherty on December 21, 2011. In response, LabMD and Daugherty moved the FTC Commissioners to quash the CID on the ground that the FTC lacked authority to issue the CID, especially because the FTC was relying upon evidence from Tiversa, a private party with a commercial interest. All but one of the FTC Commissioners denied the motion to quash. FTC Commissioner J. Thomas Rosch said in his dissent, "I do not agree that [FTC] staff should further inquire - either by document request, interrogatory, or investigational hearing - about the 1,718 File." Commissioner Rosch explained the reason for his dissent:

> Specifically, I am concerned that Tiversa is more than an ordinary witness, informant, or "whistle-blower." It is a commercial entity that has a financial interest in intentionally exposing and capturing sensitive files on computer networks, and a business model of offering its services to help organizations protect against similar infiltrations. Indeed, in the instant matter, an argument has been raised that Tiversa used its robust, patented peer-to-peer monitoring technology to retrieve the 1,718 File, and then repeatedly solicited LabMD, offering investigative and remediation services regarding the breach, long before Commission staff contacted LabMD. In my view, while there appears to be nothing per se unlawful about this evidence, the Commission should avoid even the appearance of bias or impropriety by not relying on such evidence or information in this investigation.

124. On information and belief, Sheer and Yodaiken misrepresented material facts to the Commission, failed to disclose material facts to the Commission and thereby caused the majority of the Commissioners to deny LabMD and Daugherty's motion to quash. On information and belief, Sheer and Yodaiken expressly or impliedly agreed to deprive LabMD and Daugherty of their constitutional rights by intentionally misrepresenting facts and omitting to inform their superiors and the Commissioners as follows:

- The FTC's primary "evidence" against LabMD was a file taken by Tiversa when Tiversa hacked directly into a LabMD computer;

- The only way for a user to locate the 1718 File on a peer-to-peer network was to have used the highly unusual search terms "insuranceaging" or "6.05.071";
- By accessing, downloading and retaining the 1718 File, Tiversa violated several federal and state crimes;
- The LabMD computer hacked by Tiversa was the *only* source of the 1718 File;
- When Tiversa notified LabMD it had a copy of the 1718 File, LabMD started an immediate investigation and, within minutes of its discovery of an unauthorized installation of LimeWire on one of its billing computers, removed the offending software;
- Boback and Tiversa were unreliable and not credible;
- Boback and Tiversa had manufactured evidence to make it appear that the 1718 File and files of other companies had proliferated on peer-to-peer networks when, in fact, they had not;
- Sheer, Yodaiken and Boback agreed to create a sham company to receive a CID from the FTC and that Tiversa, the actual custodian of the requested documents, was free to withhold from and provide to the FTC whatever evidence it wanted;
- There were no complaining witnesses; and
- Not one single patient suffered harm due to any alleged disclosure of the 1718 file.

125. As a result of Sheer and Yodaiken's omissions and misrepresentations to the FTC Commissioners, LabMD and Daugherty were deprived of their constitutional rights.

126. LabMD and Daugherty fought but ultimately complied with the CIDs, endured two more civil investigative hearings and produced yet more documents to Sheer and Yodaiken.

127. After years of FTC pressure and intimidation, Daugherty began speaking out regarding LabMD's ordeal with the FTC. Daugherty leveled sharp criticisms at the conduct of

the FTC in general and Sheer and Yodaiken in particular. Specifically, in early 2012, Mr. Daugherty began to warn the public about the FTC's abuses (orchestrated by Sheer and Yodaiken) through the press and social media and through a book, all to express his outrage at the way that LabMD was being treated by the federal government. Mr. Daugherty used, and continues to use, the website, http://michaeljdaugherty.com/, to criticize the government.

128. Daugherty was quoted in the September 7, 2012 edition of the Atlanta Business Chronicle saying: "We are guilty until proven innocent with these people…. They are on a fishing expedition. We feel like they are beating up on small business." The reporter wrote in her story that "Daugherty contends his company is being unreasonably persecuted by FTC. He said he's already spent about $500,000 fighting the investigation."

129. Three days later, on September 10, 2012, an FTC paralegal downloaded the Atlanta Business Chronicle article from LexisNexis and, on information and belief, disseminated it to Sheer, Yodaiken and other FTC staff members.

130. After reading Daugherty's quote, Sheer and Yodaiken ramped up their investigative efforts against Daugherty and LabMD.

131. On July 19, 2013, Daugherty posted a trailer on the internet for *The Devil Inside the Beltway*, a book he had written about his dealings with Sheer, Yodaiken and others at FTC. The trailer referred to the FTC's actions as an "abusive government shakedown" and explained that his book would "blow the whistle" about how "the Federal Trade Commission began overwhelming … [LabMD, a] small business, a cancer detection center, with their abusive beltway tactics." The trailer was especially critical of Sheer.

132. On July 22, 2013, just three days after the trailer for *The Devil Inside the Beltway* was posted on the internet, Sheer told a LabMD attorney that he and his staff recommended an enforcement action against LabMD.

The Enforcement Action

133. In their roles as Commission investigators, Defendants Sheer and Yodaiken convinced their superiors and, ultimately, the FTC Commissioners, to authorize an administrative enforcement action against LabMD. They did so by concealing the truth and misrepresenting the facts. The FTC Commissioners would not have authorized the Enforcement Action if Sheer and Yodaiken had been truthful and forthcoming with the facts. On information and belief, Sheer and Yodaiken expressly or impliedly agreed to deprive LabMD and Daugherty of their constitutional rights by intentionally misrepresenting facts and omitting to inform their superiors and the Commissioners as follows:

- The FTC's primary "evidence" against LabMD was a file taken by Tiversa when Tiversa hacked directly into a LabMD computer;
- The only way for a user to locate the 1718 File on a peer-to-peer network was to have used the highly unusual search terms "insuranceaging" or "6.05.071";
- By accessing, downloading and retaining the 1718 File, Tiversa violated several federal and state crimes;
- The LabMD computer hacked by Tiversa was the *only* source of the 1718 File;
- When Tiversa notified LabMD it had a copy of the 1718 File, LabMD started an immediate investigation and, within minutes of its discovery of an unauthorized installation of LimeWire on one of its billing computers, removed the offending software;

- Boback and Tiversa were unreliable and not credible;
- Boback and Tiversa had manufactured evidence to make it appear that the 1718 File and files of other companies had proliferated on peer-to-peer networks when, in fact, they had not;
- Sheer, Yodaiken and Boback agreed to create a sham company to receive a CID from the FTC and that Tiversa, the actual custodian of the requested documents, was free to withhold from and provide to the FTC whatever evidence it wanted;
- There were no complaining witnesses; and
- Not one single patient suffered harm due to any alleged disclosure of the 1718 file.

134. On August 28, 2013, the FTC Commissioners, relying upon Sheer and Yodaiken's misrepresentations and omissions, voted unanimously (4-0) to issue an administrative enforcement action Complaint against LabMD because LabMD had supposedly failed to provide "reasonable and appropriate security" for patient information and that this was an "unfair" act or practice in violation of Section 5.

135. The FTC filed the administrative enforcement action against LabMD on August 28, 2013 (the "Enforcement Action"). The FTC alleged that LabMD's data security practices violated unspecified standards and were "unfair" acts or practices in violation of Section 5. That same day, the FTC issued a press release and posted a blog celebrating their actions and harshly criticizing LabMD, thereby harming LabMD's public reputation.

136. Sheer was lead counsel in the Enforcement Action until the fall of 2014 when he was interviewed by the Oversight Committee in the Committee's investigation of the relationship between the FTC and Tiversa and the veracity of the information provided by Tiversa to Sheer and Yodaiken.

137. On August 29, 2013, several weeks before *The Devil Inside the Beltway* was published, the FTC issued a press release harshly criticizing LabMD. That same day, the FTC also published a "blog post" about their actions in which they made disparaging claims about LabMD and ominously framed the LabMD Complaint as a warning to other businesses: "If your clients are focused on data security —and they should be—here's a development they'll want to know about." Lesley Fair, "FTC Files Data Security Complaint Against LabMD," Business Center Blog (Aug. 29, 2013).

138. *The Devil Inside the Beltway* was published on September 24, 2013.

139. On September 30, 2013, the FTC served a subpoena on Tiversa. Tiversa failed to fully respond to the subpoena. Among other categories of documents, the subpoena requested "all documents related to LabMD." In its response, Tiversa withheld responsive information that contradicted other information it did provide about the source and spread of the 1718 File. In total, Tiversa produced 8,669 pages of documents in response to the subpoena. Because the production contained *five* copies of the 1718 File, only 79 pages of other documents remained.

140. Sheer knew that Tiversa's response to the subpoena was inadequate but took no action to compel Tiversa to fully comply with the subpoena. Sheer's purpose for serving the Tiversa subpoena was to give the appearance of independence, not to obtain evidence. In truth, Sheer had no desire to uncover any additional evidence from Tiversa, especially if the evidence was exculpatory for Daugherty and LabMD.

141. The FTC did not subpoena The Privacy Institute. That entity dissolved on or about June 18, 2013, approximately two months before the Enforcement Action began.

142. October 24, 2013, Sheer retaliated against LabMD and Daugherty by serving a subpoena on Daugherty requesting the following documents concerning Daugherty's book:

- "All drafts of … [LabMD's CEO's book about the Defendants] that were reviewed by any third party prior to the Manuscript's publication."
- "All comments received on drafts of" LabMD's CEO's book about the Defendants.
- "All documents related to the source material for drafts of" LabMD's CEO's book about the Defendants, "including documents referenced or quoted in the" book. (Complaint Counsel has defined "related" broadly to "mean discussing, constituting, commenting, containing, concerning, embodying, summarizing, reflecting, explaining, describing, analyzing, identifying, stating, referring to, dealing with, or in any way pertaining to, in whole or in part.")
- "All promotional materials related to" LabMD's CEO's book criticizing Defendants, "including, but not limited to, documents posted on social media, commercials featuring … [LabMD's CEO], and presentations or interviews given by" LabMD's CEO.

143. To punish LabMD, Sheer filed or caused to be filed burdensome, duplicative, and oppressive discovery requests that would not be allowed by an independent Article III court.

144. Sheer caused the FTC to serve LabMD's customers and other third parties, almost none of whom had anything to do with the matters at issue in the Enforcement Action, with wrongfully intrusive and burdensome subpoenas.

145. Upon information and belief, Sheer recommended the Enforcement Action to punish and to make an example of LabMD and Daugherty, both for refusing to sign consent orders and for exercising First Amendment rights to engage in constitutionally protected speech about a matter of public concern and criticize the government without fear of government reprisal.

146. One of the documents produced in the Enforcement Action by Sheer, CX0019, purports to show that Tiversa had downloaded the 1718 File from four IP addresses on particular dates and times. In truth, Tiversa analyst Wallace created CX0019, at Boback's direction, in 2013, near the time of Boback's deposition, to make it appear that the 1718 File had "spread" to IP addresses belonging to known identity thieves, and that the 1718 File had not been found at an Atlanta IP address. Boback specifically asked Wallace to include a San Diego IP address. These were lies and CX0019 was fraudulent. Sheer knew that CX0019 was fraudulent but proceeded with the evidence anyway.

147. In 2014, the Chairman of the Oversight Committee commenced an investigation of Tiversa regarding its involvement with government agencies. The investigation continued over a period of months and included investigation into Tiversa's relationship with the FTC.

148. The Oversight Committee staff report regarding its 2014 investigation concluded, inter alia, that Tiversa and Boback provided incomplete, inconsistent, and/or conflicting information to the FTC in this matter.

149. In the fall of 2014, after being interviewed by the Oversight Committee, Sheer was removed from the role of lead counsel in the Enforcement Action.

The Initial Decision

150. On November 13, 2015, Chief Administrative Law Judge D. Michael Chappell issued an Initial Decision wherein he concluded that the FTC had failed to carry its burden of proving its theory that LabMD's alleged failure to employ reasonable data security constitutes an unfair trade practice because Complaint Counsel has failed to prove the first prong of the three-part test – that this alleged unreasonable conduct caused or is likely to cause substantial injury to consumers.

151. Judge Chappell made the following findings and conclusions:

- With respect to the 1718 File, the FTC's evidence failed to prove that the limited exposure of the 1718 File has resulted, or is likely to result, in any identity theft-related harm.
- With respect to the exposure of certain LabMD "day sheets" and check copies, the FTC failed to prove that the exposure of these documents is causally connected to any failure of LabMD to reasonably protect data maintained on its computer network, as alleged in the Complaint, because the evidence fails to show that these documents were maintained on, or taken from, LabMD's computer network. In addition, the FTC failed to prove that this exposure has caused, or is likely to cause, any consumer harm.
- Judge Chappell rejected the FTC's argument that identity theft-related harm is likely for all consumers whose personal information is maintained on LabMD's computer networks, even if their information has been not exposed in a data breach, on the theory that LabMD's computer networks are "at risk" of a future data breach.
- Fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case.
- Unjustified consumer injury is the primary focus of the FTC Act.
- The Commission has stated that its "concerns should be with substantial consumer injuries; its resources should not be used for trivial or speculative harm."
- The preponderance of the evidence in this case failed to show that LabMD's alleged unreasonable data security caused, or is likely to cause, substantial consumer injury.

Accordingly, the Complaint must be dismissed, and it need not, and will not, be further determined whether or not LabMD's data security was, in fact, "unreasonable."

- Unfair conduct cases usually involve actual and completed harms.
- Historically, liability for unfair conduct has been imposed only upon proof of actual consumer harm.
- The record in this case contains no evidence that any consumer whose Personal Information has been maintained by LabMD has suffered any harm as a result of Respondent's alleged failure to employ "reasonable" data security for its computer networks, including in connection with the Security Incidents alleged in the Complaint.
- The FTC did not identify even one consumer that suffered any harm as a result of LabMD's alleged unreasonable data security.
- Given that the government has the burden of persuasion, the reason for the government's failure to support its claim of likely consumer harm with any evidence of actual consumer harm is unclear.
- Strangely, the FTC took no position as to how the Sacramento Documents came into the possession of the individuals in Sacramento, and further admits that "there is no conclusive explanation of how LabMD Day Sheets were exposed."
- The evidence shows that the 1718 File was available for peer-to-peer sharing through LabMD no earlier than June 2007 (the date of the document) until May 2008, when LabMD removed LimeWire from the billing computer.
- Although the 1718 File was available for downloading during this period, the evidence fails to show that the 1718 File was in fact downloaded by anyone other than Tiversa, who obtained the document in February 2008.

- Because of Boback's biased motive, Boback is not a credible witness concerning LabMD, the 1718 File, or other matters material to the liability of LabMD.
- Boback was evasive and lacked forthrightness in response to questioning during his June 7, 2014 video deposition taken by LabMD for purposes of trial testimony.
- Boback's testimony in this case is not credible.
- Boback's 2013 discovery deposition, Boback's 2014 trial deposition testimony, and a Tiversa-provided exhibit, CX0019, are unreliable, not credible, and outweighed by credible contrary testimony from Wallace.
- Tiversa's Data Store is not a credible or reliable source of information as to the disclosure source or the spread of any file purportedly found by Tiversa.
- Former Commissioner Rosch advised in April 2012, in his dissenting opinion on LabMD's Motion to Quash or Limit Civil Investigative Demand, that, under these circumstances, the FTC staff should not inquire about the 1718 File, and should not rely on Tiversa for evidence or information, in order to avoid the appearance of impropriety. Judge Chappell noted FTC staff did not heed then-Commissioner Rosch's warning, and also did not follow his advice. Instead, Complaint Counsel chose to further commit to and increase its reliance on Tiversa.

152. Sheer, Yodaiken, Settlemyer, Boback and Tiversa have won. Through the Federal Defendants' abuses of power and disregard for the core constitutional rights of LabMD and Daugherty, the Federal Defendants have put LabMD out of business and laid it to rest. In addition, they have deprived Daugherty of his right to make a living from an extremely valuable asset that he built from the ground up.

CLAIMS FOR RELIEF

COUNT I
(Constitutional Violation – First Amendment, Freedom of Speech)
(All Defendants)

153. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 152 above, as if fully set forth verbatim in this Count I.

154. Federal Defendants negligently, intentionally and willfully abridged Daugherty and LabMD's constitutional rights to express their information, thoughts, opinions, beliefs, ideas and creativity and other protections and violated Plaintiffs' other rights and privileges in the First Amendment.

155. As a result of the Federal Defendants violation of Plaintiffs' constitutional rights, Plaintiffs have been harmed in amounts to be proven at trial.

COUNT II
(Constitutional Violation – First Amendment, Freedom of the Press)
(All Defendants)

156. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 155 above, as if fully set forth verbatim in this Count II.

157. The Federal Defendants negligently, intentionally and willfully abridged Daugherty and LabMD's constitutional rights to publish their information, thoughts, opinions, beliefs, ideas and creativity and violated Plaintiffs' other rights and privileges in the First Amendment.

158. As a result of the Federal Defendants violation of Plaintiffs' constitutional rights, Plaintiffs have been harmed in amounts to be proven at trial.

COUNT III
(Constitutional Violation – First Amendment, Right to Petition Government for Redress of Grievances)
(All Defendants)

159. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 158 above, as if fully set forth verbatim in this Count III.

160. The Federal Defendants negligently, intentionally and willfully abridged Daugherty and LabMD's constitutional rights to petition their government and elected officials for redress of their concerns and grievances and violated Plaintiffs' other rights and privileges in the First Amendment.

161. As a result of the Federal Defendants violation of Plaintiffs' constitutional rights, Plaintiffs have been harmed in amounts to be proven at trial.

COUNT IV
(Constitutional Violation – Fourth Amendment, Unreasonable Search and Seizure)
(All Defendants)

162. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 161 above, as if fully set forth verbatim in this Count IV.

163. The Federal Defendants negligently, intentionally and willfully abridged Daugherty and LabMD's constitutional rights against unlawful search and seizure and violated Plaintiffs' other rights and privileges in the Fourth Amendment.

164. As a result of the Federal Defendants violation of Plaintiffs' constitutional rights, Plaintiffs have been harmed in amounts to be proven at trial.

COUNT V
(Constitutional Violation – Fifth Amendment, Procedural Due Process)
(All Defendants)

165. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 164 above, as if fully set forth verbatim in this Count V.

166. The Federal Defendants negligently, intentionally and willfully abridged Daugherty and LabMD's constitutional rights to procedural due process and violated Plaintiffs' other rights and privileges in the Fifth Amendment.

167. As a result of the Federal Defendants violation of Plaintiffs' constitutional rights, Plaintiffs have been harmed in amounts to be proven at trial.

COUNT VI
(Constitutional Violation – Fifth Amendment, Substantive Due Process)
(All Defendants)

168. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 167 above, as if fully set forth verbatim in this Count VI.

169. The Federal Defendants negligently, intentionally and willfully abridged Daugherty and LabMD's constitutional rights to substantive due process and violated Plaintiffs' other rights and privileges in the Fifth Amendment.

170. As a result of the Federal Defendants violation of Plaintiffs' constitutional rights, Plaintiffs have been harmed in amounts to be proven at trial.

COUNT VII
(Civil Conspiracy under Federal Common Law)
(All Defendants)

171. Daugherty and LabMD re-allege and incorporate all of the allegations set forth in Paragraphs 1 through 170 above, as if fully set forth verbatim in this Count VII.

172. The Federal Defendants expressly and impliedly agreed among themselves to deprive Plaintiffs of their constitutions rights.

173. The Federal Defendants actually deprived Plaintiffs of their constitutional rights as a result of their express and implied agreements.

PRAYER FOR RELIEF

WHEREFORE, Daugherty and LabMD respectfully demands the following relief:

a) That Daugherty and LabMD recover from and have judgment against Federal Defendants, sued in their individual capacities, jointly and severally, in such sums as sufficient to fully compensate Plaintiffs for all of their damages, losses and injuries sustained as a result of the facts set forth above, including, without limitation, consequential, general, nominal and special damages as well as punitive damages in amounts to be determined by the enlightened conscience of the jury;

b) For an award of reasonable attorneys' fees and costs against Federal Defendants; and

c) For such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiffs seek a trial by jury of all issues so triable.

Dated: November 20, 2015

Respectfully submitted,

/s/Jason H. Ehrenberg

Jason H. Ehrenberg (#469077)
Peter K. Tompa (#413752)
BAILEY & EHRENBERG PLLC
1015 18th Street, NW
Suite 204
Washington, DC 20036
Phone: 202.331.4209
Facsimile: 202.318.7071
jhe@becounsel.com

and

James W. Hawkins
Pro hac vice (application to be filed)
Georgia State Bar No. 338767
JAMES W. HAWKINS, LLC
11339 Musette Circle
Alpharetta, GA 30009
V: 678-697-1278
F: 678-540-4515
jhawkins@jameswhawkinsllc.com

Attorneys for Plaintiffs Michael J. Daugherty and LabMD, Inc.