**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF NEW YORK**

| | | |
|---|---|---|
| UNITED STATES OF AMERICA *ex rel.* **[UNDER SEAL]**, | : | Civil Action No. _____ |
| | : | |
| | : | Judge _____ |
| Plaintiff and Relator, | : | |
| | : | |
| v. | : | |
| | : | **FILE UNDER SEAL** |
| **[UNDER SEAL]** | : | Pursuant to 31 U.S.C. |
| | : | § 3730(b)(2) |
| | : | |
| Defendants. | : | |
| | : | |
| | : | |
| | : | **DO NOT SERVE** |
| | : | |

**COMPLAINT FOR VIOLATIONS OF THE FALSE CLAIMS ACT**

**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF NEW YORK**

| | | |
|---|---|---|
| UNITED STATES OF AMERICA *ex rel.* Michael J. Daugherty, | : | Civil Action No. _____ |
| | : | |
| | : | Judge _____ |
| Plaintiff and Relator, | : | |
| | : | |
| v. | : | |
| | : | **FILE UNDER SEAL** |
| TIVERSA HOLDING CORP., | : | Pursuant to 31 U.S.C. |
| TIVERSA GOVERNMENT INC., | : | § 3730(b)(2) |
| TIVERSA INC., AND ROBERT BOBACK, | : | |
| | : | |
| Defendants. | : | **DO NOT SERVE** |
| | : | |

**COMPLAINT FOR VIOLATIONS OF THE FALSE CLAIMS ACT**

## I. INTRODUCTION.

1. *Qui tam* Relator Michael J. Daugherty brings this action on his own behalf and on behalf of the United States of America to recover damages and penalties under the False Claims Act, 31 U.S.C. § 3729 *et seq.*, against Defendants Tiversa Holding Corp., Tiversa Government, Inc., and Tiversa Holding Corp.'s predecessor Tiversa Inc. (collectively "Tiversa") and Tiversa's Chief Executive Officer Robert J. Boback ("Boback").

2. This case arises out of Defendants' scheme to defraud the United States Government by submitting or causing submission of false or fraudulent claims for payment to the United States.

3. Defendants routinely make false representations to federal entities in order to induce those entities to award lucrative contracts to Defendants. Specifically, Defendants search peer-to-peer ("P2P") computer networks in order to identify and seize sensitive information inadvertently made available by someone within or related to a public entity who has downloaded P2P software. Defendants then contact that entity and falsely represent that the

entity has a security breach of unknown origins or scope, and needs Tiversa's services to identify the breach. To further the urgency for Tiversa services, Defendants also identify Internet Protocol ("IP") addresses of known bad actors, such as identity thieves and other criminals, where it would be particularly problematic for sensitive information to be found. Defendants then falsely claim that Tiversa found copies of the identified file at those addresses.

4. Having created the fictitious problem, Tiversa then sells its security services to fix the fabricated "problem." It is a classic protection racket, updated for the digital age.

5. Defendants' scheme has been employed on public and private entities nationwide, to include at least the Department of Homeland Security; the Transportation Security Administration; the Department of Defense; the Patent and Trademark Office; the Department of the Treasury; the Department of Education; the House of Representatives; and various government contractors.

6. Upon information and belief, these practices have been employed to deceive federal entities into entering into contracts with Tiversa since its inception in 2004, and is ongoing.

7. Defendants' scheme falsely induces Government entities to enter into contracts with Tiversa. Once these contracts are obtained, Defendants continue to falsely represent to the contracted entity that Tiversa's services are needed, often through the continued falsification of alarming breaches.

8. Defendants' scheme has resulted in false claims for payment to the Government and millions of dollars in falsely procured services.

## II. JURISDICTION AND VENUE.

9. This action arises under the United States Civil False Claims Act, 31 U.S.C. § 3729 *et seq*.

10. The Court has subject-matter jurisdiction pursuant to 31 U.S.C. § 3732(a) and 28 U.S.C. § 1331, and has personal jurisdiction over Defendants because they transact business in this District.

11. Venue in this District is proper under 28 U.S.C. 1391(b) and (c), and 31 U.S.C. 3732(a).

12. The facts and circumstances regarding the fraud on Government entities alleged in this complaint have not been publicly disclosed in a federal criminal, civil, or administrative hearing in which the Government or its agent is a party; or in a Congressional, Government Accountability Office, or other federal report, hearing, audit, or investigation; or in the news media.

13. In the event of a public disclosure, Relator is an original source of the information upon which this complaint is based, as that phrase is used in the False Claims Act. He has knowledge that is independent of and materially adds to any publicly disclosed allegations or transactions, and he has disclosed the facts upon which this action is based to the United States prior to the filing of this complaint.

## III. PARTIES.

14. The real party in interest to the claims set forth herein is the United States of America.

15. Relator Michael Daugherty is a resident of Georgia. Mr. Daugherty received his undergraduate degree in Economics from the University of Michigan in 1982. Since that time,

Mr. Daugherty has worked in a variety of roles within the medical profession, and in 1996, Mr. Daugherty founded a urology health center, ultimately called LabMD, a full-service uropathology and microbiology cancer-detection laboratory. Mr. Daugherty is the former President of LabMD. LabMD was forced to close in 2014 because of financial difficulties caused in substantial part by Defendants' fraud scheme.

16. Defendants Tiversa Holding Corp. and Tiversa Government Inc. are Delaware corporations, each formed on March 29, 2012. Defendant Tiversa Holding Corp.'s predecessor company Tiversa, Inc. was a Pennsylvania corporation formed on January 15, 2004, and merged into Tiversa Holding Corp. on April 10, 2012. Collectively, Defendants are referred to as "Tiversa," with a principal place of business at 606 Liberty Ave., Pittsburgh, Pennsylvania 15222. Tiversa is a global company that specializes in internet data protection and review.

17. Defendant Robert J. Boback is a resident of Pennsylvania and is a co-founder and the Chief Executive Officer of Tiversa.

## IV. RULE 9(b), FED. R. CIV. P., ALLEGATIONS.

18. Much of the documentary evidence necessary to prove the allegations in this Complaint is in the exclusive possession of either the Defendants or the United States, and on information and belief, some evidence is classified.

19. With respect to each allegation herein made upon information and belief, Relator has, based upon his knowledge, data, and experience, a reasoned factual basis to make the allegation but lacks complete details of it.

20. Relator is familiar with Defendants' policies and procedures from his experience of having been a victim of those policies and procedures and from his investigation into the tactics and schemes of Defendants.

## V. FACTS.

### A. OUTLINE OF THE SCHEME.

21. P2P networks are a method of distributing files over the internet.

22. In contrast to file-sharing methods such as electronic mail, instant messaging, and websites, which allow users to download content from a central server, P2P networks have no server. Rather, the defining characteristic of a P2P network is that users' computers communicate directly with each other.

23. In order to access P2P networks such as Gnutella or FastTrack, users must download software that enables them to, over the internet, search for and retrieve files located in shared folders on the computers of other users who participate in the network. Well-known examples of P2P software include Limewire and KaZaA. Typically, P2P file-sharing networks are accessible to anyone using the right software.

24. P2P networks have been controversial for many years, initially because of the ease with which copyrighted music and video files could be shared in violation of copyright laws.

25. By 2003, concerns about the risks of inadvertent file-sharing had reached the point where Congress felt compelled to act, and the House passed the Government Network Security Act of 2003. Although it stalled in the Senate, the bill would have required government agencies to create policies and procedures to protect government computers from the security risks posed by file-sharing via P2P networks.

26. By its nature, P2P file-sharing is diffuse, and any individual user can download and install P2P software for seemingly-benign uses. Therefore, ensuring the privacy of information on computers that are connected to P2P networks has been an ongoing challenge.

27. Tiversa markets itself to federal entities and private companies as "the industry leader…on processes and strategy to address the risks associated with file-sharing." It represents that it "detects, locates and identifies exposed files in real-time, while assisting in remediation and prevention efforts." In short, it finds the problem and sells the solution.

28. Tiversa publicly touts that it is the sole-source vendor for the Department of Homeland Security and that it provides "protection and intelligence to global law enforcement, government agencies and defense contractors." Its marketing approach has been quite successful for the company, resulting in revenues believed to exceed $10 million each year in Government contracts alone.

29. The scheme is relatively simple, but it is cloaked in the complexity of computer programs, metadata, and P2P networks.

30. First, Tiversa finds a potential victim. Using proprietary software, Tiversa identifies files containing sensitive information that have been made vulnerable to viewing via a P2P network or application. Somewhere, and typically by accident, a user has made a sensitive file vulnerable to being viewed by others via a P2P network or application. Tiversa finds such files either by performing searches using key words it knows will be found in such files (for example, "Social Security number" or "tax return"), or by monitoring traffic on the P2P networks and piggybacking on searches conducted by others that might return sensitive files.

31. Once it identifies a sensitive file, Tiversa exploits the general lack of knowledge about P2P, the generalized fear about the exposure of private information, and its exclusive use of its proprietary software to sell its security services to the exposed party, including Government entities.

32. Should the victim decline to take Tiversa's bait, Tiversa ups the ante by lying about the file. Tiversa knows that the file was found on just one computer—often a computer of an employee at the targeted entity who has downloaded P2P software to share music with others—through a gap that could easily be closed by uninstalling the software from the affected machine. Yet, per Boback's direction, Tiversa does not disclose to targeted individuals and entities that the file is only identified on the target's own computer and that the vulnerability is easily remediable.

33. Rather, Tiversa claims that the sensitive information has spread, often world-wide. Tiversa identifies IP addresses of known criminals, to include child pornographers and identity thieves, or of computers in countries considered adverse to the interests of the United States, to include Iran, Pakistan and China. Tiversa informs its target entity that it found copies of the identified file at those addresses. In short, it claims not only that a sensitive file (such as a classified or patient-protected file) is vulnerable, but that the information has been seized and seen by others with likely nefarious motives.

34. If forced to identify the stolen data for a targeted entity, Boback directs Tiversa employees to strip the found file of all identifying metadata (e.g., the original author of the file, the time and date it was created) before sharing it with a target in order to increase the sense that the target company needs Tiversa's help, even to identify the file itself.

35. Instead of disclosing the true metatdata associated with the file, Boback directs employees to physically modify the files it obtains over the P2P network to falsely show that the files were pulled from other IP addresses, in order to support Tiversa's claims that the file has "spread" over the internet. The altered files are then deposited into Tiversa's datastores.

36. The exposed party, understandably disturbed by the apparent global spread of its sensitive data and hamstrung by Tiversa's efforts to conceal the truth, buys Tiversa's services on the false premise that the targeted entity's security has been breached and that Tiversa is the entity's only hope going forward.

37. In reality, Tiversa merely found a vulnerable file, but, until Tiversa came along, the file had not actually yet been viewed or accessed by anyone other than its original host. The assertion that Tiversa found the file at other sites is false. There had been no seizing by others, nefarious or otherwise.

38. That the private information was accessed and disseminated is a critical component of Tiversa's marketing plan, and it is a critical reason why Government entities and others contract with Tiversa for security services. But it is a lie.

39. Tiversa's lies falsely induce Government entities to contract with it. Tiversa continues the lie once the contract has been gained, accepting payment for false protection services.

40. After having some of these targeted entities cancel contracts after a period of time, Boback instructed Tiversa employees to fabricate new breaches, in order that the contracting entities would continue to use Tiversa services.

41. Defendants' false representations resulted in false claims to the United States.

**B. EXAMPLES OF FALSE REPRESENTATIONS.**

**1. LABMD: FALSE REPRESENTATIONS ABOUT HIPAA DISCLOSURES.**

42. Relator's company, LabMD, was a victim of Tiversa's scheme. While LabMD was a private healthcare entity that ultimately refused to contract with Tiversa (at significant

consequence), Tiversa's false representations regarding LabMD are representative of the false scheme employed by Defendants.

43. On or about May 13, 2008, Boback contacted LabMD and told the company that Tiversa had a LabMD file containing over 1,700 pages of patient health information.

44. Relator asked Boback to provide details regarding the file and how Tiversa had come to find it. A Tiversa employee responded that day, stating that Tiversa had first downloaded the file on February 5, 2008, that Tiversa did not attempt to download it again, and that Tiversa's system did not auto-record the IP address but they could likely find that information.

45. Boback refused to provide additional details until Relator signed a contract with Tiversa.

46. All subsequent attempts by Relator to glean additional information about how Tiversa accessed the LabMD file were met with essentially the same response: "we won't tell you anything now, but we can help you if you hire us."

47. Over the ensuing months, Boback repeatedly contacted LabMD in an attempt to coerce it into hiring Tiversa. LabMD repeatedly refused.

48. Upon being informed that its file had been found on a P2P network, LabMD immediately identified the employee's computer that had P2P software installed and removed both the software and the file from the computer. LabMD also then conducted a search of P2P networks and determined that the file was no longer accessible. LabMD engaged a third-party vendor to examine the integrity of its data security systems.

49. In April or May of 2009, Tiversa met with attorneys with the Federal Trade Commission (the "FTC") in Pennsylvania. At that meeting, the FTC attorneys asked Tiversa for

a list of companies that had files available via P2P networks that contained greater than one hundred disclosures of names, Social Security numbers, or other personal identifiers.

50. Tiversa created a separate legal entity for the purposes of receiving an FTC Civil Investigative Demand ("CID") for the information. On June 6, 2009, an entity called the Privacy Institute was created, and shortly thereafter was served with the CID.

51. Tiversa generated the list of companies requested by the FTC. That list, a spreadsheet ultimately called "FTC List 71609," included, among files linked to 96 other companies, the LabMD file. The list was not, however, reflective of all companies known to Tiversa that had exposed files containing over 100 identifiers: Before Tiversa provided the list to the FTC, Boback directed an employee to scrub the list of then-current clients because he did not want to jeopardize Tiversa's client relationships. Thus, Tiversa did not turn over information regarding clients which had paid for ongoing protection.

52. On or about August 18, 2009, the Privacy Institute responded to the FTC's Civil Investigative Demand and, *inter alia*, produced the list of companies identified in the "FTC 71609" spreadsheet, as well as the LabMD file.

53. In approximately late 2009, FTC attorneys requested additional information from Tiversa regarding the spread of the LabMD file. Upon information and belief, Tiversa engaged in discussions with the FTC about how Tiversa would be reimbursed for its services in providing additional information.

54. After those discussions were complete, and an arrangement was finalized about how information would be provided, Tiversa provided additional information to the FTC.

55. Specifically, in approximately the summer of 2010, Boback directed a Tiversa employee to falsify the spread of the LabMD file in order to create the false appearance that the

LabMD file had spread beyond its host. He instructed the employee to make sure that he linked the file to known "bad guys."

56. That Tiversa employee, under Boback's instruction and supervision, identified three IP addresses of known identity thieves or child pornographers and created a document indicating that the LabMD file had been found at those IP addresses. That document also included the IP address of the LabMD computer where the file was actually found.

57. Defendants provided that information to the FTC, falsely asserting that the LabMD file was found at four IP addresses, when in reality it was only found at the host address.

58. To substantiate the lie that the file's distribution had spread beyond only its host, Boback instructed Tiversa's employee to falsify the metadata on the file and to create an internal company file that would support the assertion that the file was found at the addresses identified to the FTC.

59. At Boback's direction, the employee used file-renaming software to alter the metadata of the LabMD file. He then deposited that altered version of the LabMD file into Tiversa's internal datastore (using Tiversa's network administrator, as was Tiversa's practice) where Tiversa stores the files it downloads from its P2P searches. At Boback's direction, the altered LabMD file was deposited into Tiversa datastore subfolders linked to the three IP addresses of "bad guys." Those subfolders already contained documents that had actually been found at those IP addresses, and the Tiversa employee simply altered the subfolder information in order to create the appearance that the LabMD file was found at that IP address at a specific time and date that corresponded to the story Tiversa wanted to tell about the LabMD file. Tiversa's datastores are re-indexed nightly, so that by the next day, the files appeared in the order of their new, false dates.

60. On August 29, 2013, the FTC filed an administrative complaint against LabMD, alleging that LabMD failed to reasonably protect the security of consumers' data.

61. In approximately October 2013, when it appeared to Boback that it would be advantageous to Tiversa to show that the LabMD file had never been found at its host and that, instead, it had been found originally in California, Boback caused Tiversa's employee to add another IP address to the list of addresses where the LabMD file had supposedly been found: a San Diego, California IP address that was provided to the employee by Boback. Boback then instructed that employee to create a second operative list of the IP addresses where the LabMD file was falsely claimed to have been found; the new list of four addresses included the San Diego address instead of the actual LabMD Atlanta address. An altered version of the LabMD file was then inserted into Tiversa's datastore in a folder linked to the San Diego IP address provided by Boback.

62. The FTC-LabMD administrative action has been in active litigation since 2013. Boback has testified twice in that litigation, and has falsely testified as to the source of the original disclosure of the LabMD file.

63. The FTC litigation is not the only place where Defendants used false representations about the LabMD file for its own gain.

64. On information and belief, the United States Department of Homeland Security ("DHS") awarded a multi-million-dollar grant in 2006, Award Number 2006-CS-001-000001, to Dartmouth College, as part of DHS's cyber-security initiatives.

65. On or about February 22, 2009, M. Eric Johnson of the Center for Digital Strategies at the Tuck School of Business at Dartmouth College published "Data Hemorrhages in the Health-Care Sector," in a publication entitled "Financial Cryptography and Data Security:

13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers." The research detailed in that paper was supported by that DHS grant; the federally-funded study analyzed the consequences of files leaked over internet file-sharing networks.

66. Dartmouth publically represented, including to DHS, that it engaged the services of Tiversa to conduct a targeted search of the top-ten publically traded healthcare firms and then to conduct a refined search of host computers where Tiversa found sensitive information in that first stage.

67. Dartmouth represented that the LabMD file was found pursuant to those parameters. An excerpt of the LabMD file provided by Tiversa features prominently in Mr. Johnson's paper as an example of the type of information Tiversa found during the DHS-funded study.

68. In reality, however, the LabMD file was not found during the DHS-funded study; it was instead found during Tiversa's routine trolling of the P2P networks in its pursuit of potential victims for its scheme.

69. Recipients of DHS grants are required to submit timely, complete, and accurate reports to DHS. For the period January 1 – March 31, 2009, Dartmouth made a required quarterly report to DHS on Initiative 5: Business Rationale for Cyber Security, which was one of the projects funded by the 2006 Award. In that report, Dartmouth touts Johnson's 2009 article as evidence of its performance under the grant.

70. Defendants' misrepresentations to Dartmouth regarding the identification of data in support of study protocols caused Dartmouth to make false representations to DHS in support of its receipt of DHS grant funds.

71. Tiversa actively marketed the DHS-study in the promotion of its own services. *E.g.*, May 28, 2009 Press Release by Tiversa, http://www.tiversa.com/learningcenter/newsroom/media/press/2009/2009_05_28_Tiversa_Identifies_Over_13Million.html.

**2. MARINE ONE.**

72. Marine One is the call sign used to identify any helicopter used by the Marine Corps to transport the President of the United States. In 2009, Defendant Boback appeared on national media and before two different congressional committees, asserting a "national security risk" created by the disclosure of the Marine One flight plan, which he testified and told interviewers that Tiversa had found on a workstation in Iran.

73. On May 5, 2009, Boback testified before the House Subcommittee on Commerce, Trade and Consumer Protection, stating: "In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran."

74. What neither Congress nor the public ever knew, however, was that the information was not "apparently downloaded" by anyone in Iran. Instead, Boback instructed an employee to find an IP address in Iran that could be used to perpetuate that lie. The employee did identify such an address, and Boback proceeded to twice falsely testify before Congress that Marine One's information was found there.

75. Boback's false testimony resulted in ongoing work with the House Oversight and Government Reform Committee to provide it with evidence to buttress the Committee's attempt to ban the use of P2P technology on government computers.

76. At that May 2009 hearing, Boback provided an excerpt of the LabMD file to the Subcommittee as an example of sensitive information being made available via P2P networks.

### C. DEFENDANTS' KNOWING SCHEMES RESULTED IN FALSE CLAIMS TO THE UNITED STATES.

77. At all times, Defendants acted knowingly to submit or cause to be submitted false claims to the United States.

78. Defendants' scheme of lying about how and where Tiversa finds sensitive files has been employed against numerous Government entities both to secure Government contracts and during the performance of such contracts in order to induce the entities to continue the contracts. These entities include, without limitation, the Department of Homeland Security; the Transportation Security Administration; the Department of Defense; the U.S. Patent and Trademark Office; the Department of the Treasury; the Department of Education; the United States House of Representatives; and various Government contractors. On information and belief, many of the contracts at issue are classified.

79. By falsely representing that sensitive information was found on computers where such information was not, in fact, found, Defendants made material, false representations to the United States in order to fraudulently induce Government entities to contract with Tiversa for its data-security services. Every payment made by the Government pursuant to those fraudulently-induced contracts is the result of a false claim.

80. Defendants continue their fraud in order to ensure that its federal contracts continue and are renewed. Thus, in the provision of their data-security services to Government entities with which they have contracts, Defendants continue to falsely disclose potential breaches of sensitive information. Defendants ensure that the contracted entities continue to

have the impression that Tiversa services are needed, and never reveal that the initial breach was an easily remediable vulnerability on an individual workstation.

81. Defendants' fraudulent representations to Government entities go to the core of the conditions of the contract, and all resulting claims under those contracts are false claims.

82. Defendant Boback knowingly instigated, led, and directed the fraud detailed herein. Not only did he falsely testify on at least two occasions before congressional committees, he personally directed Tiversa employees to find IP addresses to which Tiversa could and did attribute the finding of sensitive information in order to secure contracts with the victims. He knowingly used, or directed the use of, fabricated information to fraudulently induce Government agencies and divisions to contract with Tiversa and then to maintain the contracts.

83. Boback also used each new contract to induce more contracts with Government entities. Boback propagated the false representation that he and his company had provided necessary and urgently-needed cyber-protection services to the Government, when in fact those services and any attendant credibility were built on a straw man of false representations.

84. Boback's false representations regarding national security leaks and other serious data breaches gained significant media attention. Boback promoted increasing media attention to these falsehoods, to induce public and private entities to contract with Tiversa.

85. The Government has been damaged by Defendants' conduct, to include all payments made by the Government as a result of these false representations, including the cost of fraudulently induced and fraudulently performed contracts.

**COUNT I**
**Violations of the False Claims Act, 31 U.S.C. § 3729(a)(1)**

86. The allegations in the foregoing paragraphs are re-alleged as if fully set forth below.

87. This is a civil *qui tam* action brought by relator on behalf of the United States to recover treble damages and civil penalties under 31 U.S.C. § 3729(a) of the False Claims Act.

88. The False Claims Act imposes liability on any person who (A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval; or (B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim. 31 U.S.C. § 3729(a)(1).

89. By virtue of the above-described acts, among others, every claim for payment submitted by a defendant to any federal agency with which it obtained a contract after making false representations about locations where files were found was false or fraudulent, and Defendants violated 31 U.S.C. § 3729(a) by knowingly presenting or causing to be presented, to officers or employees of the United States, including a member of any agency thereof, these false or fraudulent claims for payment.

90. By virtue of the above-described acts, among others, Defendants violated 31 U.S.C. § 3729(a) because they knowingly made, used, or caused to be made or used, false records or statements material to a false or fraudulent claim.

91. Defendants acted knowingly, as that term is used in the False Claims Act.

92. The United States, unaware of the falsity of the records, statements, and claims made or caused to be made by Defendants, paid and continues to pay the claims that would not be paid but for Defendants' illegal conduct.

93. The United States Government has been damaged, and continues to be damaged, as a result of Defendants' conduct in violation of the False Claims Act in an amount to be determined at trial.

## PRAYER FOR RELIEF

WHEREFORE, Relator requests:

A. That the Court enter judgment against the Defendants in an amount equal to three times the amount of damages the United States Government has sustained because of Defendants' actions, plus a civil penalty of $11,000 for each action in violation of 31 U.S.C. § 3729, and the costs of this action, with interest, including the costs to the United States Government for its expenses related to this action;

B. That in the event the United States Government intervenes in this action, Relator be awarded 25% of the proceeds of the action or the settlement of any such claim;

C. That in the event the United States Government does not proceed with this action, Relator be awarded 30% of the proceeds of this action or the settlement of any such claim;

D. That Relator be awarded all costs, attorneys' fees, and litigation expenses; and

E. That the United States Government and Relator receive all relief, both at law and in equity, to which he may reasonably appear entitled.

Respectfully submitted,

Jennifer M. Verkamp (*pro hac vice* to be filed)
Frederick M. Morgan, Jr. (*pro hac vice* to be filed)
MORGAN VERKAMP LLC
35 East 7th St., Suite 600
Cincinnati, OH 45202
Telephone: (513) 651-4400
Fax: (513) 651-4405
Email: jverkamp@morganverkamp.com
rmorgan@morganverkamp.com

David A. Koenigsberg
MENZ BONNER KOMAR & KOENIGSBERG LLP
444 Madison Ave., 39th Floor
New York, NY 10022
Telephone: (212) 223-2100
Facsimile: (212) 223-2185
dkoenigsberg@mbkklaw.com

*Counsel for Relator*

**DO NOT SERVE ON DEFENDANTS**

**SEALED FALSE CLAIMS ACT COMPLAINT**