UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF KANSAS

UNITED STATES OF AMERICA EX REL [UNDER SEAL],	Case No. 16-2034 CM/JPO
Plaintiffs,	**FILED UNDER SEAL PURSUANT TO 31 U.S.C. §3730(B)(2)**
v.	**DO NOT PLACE IN PRESS BOX DO NOT ENTER ON PACER**
[UNDER SEAL],	
Defendant.	COMPLAINT FOR DAMAGES UNDER THE FEDERAL FALSE CLAIMS ACT
	DEMAND FOR JURY TRIAL

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF KANSAS

UNITED STATES OF AMERICA EX REL BASHAR SEAN AWAD and CYNTHIA MCKERRIGAN, Plaintiffs, v. COFFEY HEALTH SYSTEM, Defendant.	Case No. **FILED UNDER SEAL PURSUANT TO 31 U.S.C. §3730(B)(2)** **DO NOT PLACE IN PRESS BOX** **DO NOT ENTER ON PACER** COMPLAINT FOR DAMAGES UNDER THE FEDERAL FALSE CLAIMS ACT DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Qui Tam plaintiffs Bashar Sean Awad ("Relator Awad") and Cynthia McKerrigan ("Relator McKerrigan") (collectively "Relators"), through their counsel, bring this action on behalf of the United States of America, under the False Claims Act ("FCA"), 31 U.S.C. §3729, *et seq.*, based upon personal knowledge, relevant documents, and information and belief, and in support thereof, state and allege as follows:

I. NATURE OF THIS ACTION

1. This action is based on false claims being submitted by Coffey Health System ("Coffey" or "Defendant") from or about 2011 or 2012 to the present. The false claims were submitted by Coffey to the United States of America, through Medicare and Medicaid, for incentive payments regarding electronic health records ("EHR"), resulting in substantial damages to the United States of America.

2. **False Security Attestations:** More specifically, from about 2011 or 2012 to the present, Coffey has been falsely attesting to Medicare and Medicaid that it is in compliance with certain security standards, as required by law, which was a required attestation prior to being eligible to receive EHR incentive payments from Medicare and Medicaid, and which caused Medicare and Medicaid to wrongfully pay Coffey at least $3 million in incentive payments.

3. **False Data Attestations:** Similarly, from about 2014, or earlier, to the present, Coffey also falsely attested that the data it submitted to Medicare and Medicaid was captured and exported from its EHR technology, when in fact it was not; rather, it was captured and exported manually, not by Coffey's EHR technology.

4. But for Defendant's false security attestations and false data attestations, Coffey would have never received the at least $3 million in incentive payments that it did, from the government.

5. Defendant, by its unlawful conduct of knowingly submitting false claims to the government, for payment of government funds, has violated the FCA, and is liable to the government, for treble damages and penalties associated with the false claims alleged herein.

II. JURISDICTION AND VENUE

6. This is an action to recover damages and civil penalties on behalf of the United States of America arising out of false claims, transactions, and other related acts of Defendant, and is brought pursuant to 31 U.S.C. §§3729-3733, more popularly known as the FCA, through Relators, pursuant to 31 U.S.C. §3730(b), for and on behalf of the United States of America.

7. Jurisdiction of the Court is founded upon 28 U.S.C. §§1331 and 1345. The claims set forth herein arise under and are founded upon federal law. Relators are aware of no jurisdictional bars to this action.

8. Personal jurisdiction over Defendant is proper in this Court pursuant to 31 U.S.C. §3732(a), which provides that any action under 31 U.S.C. §3730 may be brought in any district in which the defendant can be found, resides, transacts business, or in which any act proscribed by 31 U.S.C. §3729 occurred.

9. Venue is proper in this District pursuant to 31 U.S.C. §3732(a) and 28 U.S.C. §1391(b). Defendant is found in and transacts business in the state of Kansas, including the conduct which gives rise to the fraudulent claims set forth herein.

III. PARTIES

10. ***The United States of America*** is the real plaintiff in interest with respect to the claims asserted herein. Medicare and Medicaid (hereinafter often collectively referred to, for the save of convenience, as "Medicare") are federal programs[1] of the United States of America and are administered and supervised by the Centers for Medicare & Medicaid Services ("CMS"), a division of the United States Department of Health & Human Services ("HHS").

11. ***Relator Awad*** is a resident of Overland Park, Johnson County, Kansas. From about August 2014 to about July 2015, Relator Awad was the Chief Information Officer ("CIO") of Defendant and worked with Coffey's executive management team in defining custom reports and designing custom analytics. Relator Awad's personal knowledge, beliefs, and experiences,

[1] The Medicaid program is jointly funded by the federal government and states.

based mainly on his employment at Coffey, are consistent with the allegations discussed herein.

12. ***Relator McKerrigan*** is a resident of Topeka, Shawnee County, Kansas. Relator McKerrigan is a former employee of Defendant; she was the Corporate Compliance Officer and Grant Writer for Defendant from July 7, 2014, until she ended her employment with Coffey around December 2014. Relator McKerrigan's personal knowledge, beliefs, and experiences, based mainly on her employment at Coffey, are consistent with the allegations discussed herein.

13. ***Defendant Coffey*** is a non-profit system that provides health care in the state of Kansas. Coffey is considered a component unit of Coffey County, Kansas. The Coffey County Board of County Commissioners appoints members to the Board of Trustees of Coffey, each of whom serve three year terms. In addition to its Coffey County Hospital location which provides acute health care, Coffey operates a home health agency, five physician clinics, and two long-term care facilities, which in total, employ roughly 300 people. Coffey's registered office of record is its Coffey County Hospital location at 801 N. 4th Street, Burlington, Kansas.

IV. BACKGROUND ALLEGATIONS

A. The FCA—Generally

14. The FCA prohibits several variations of fraud on the government.

15. Among other things, the FCA prohibits knowingly presenting, or causing to be presented, to the federal government a false or fraudulent claim for payment or approval, and conspiring to defraud the government by getting a false or fraudulent claim allowed or paid. 31 U.S.C. §3729(a)(1)(A).

16. Additionally, the FCA prohibits knowingly making or using, or causing to be made or used, a false or fraudulent record or statement to get a false or fraudulent claim paid or approved by the federal government. 31 U.S.C. §3729(a)(1)(B).

17. The FCA defines "knowing" as acting with a deliberate ignorance of, or reckless disregard of, the truth or falsity of the information. 31 U.S.C. §3729(b).

18. The statute allows any person having information about an FCA violation to bring an action on behalf of the United States of America and to share in any recovery obtained. It

requires that the complaint be filed under seal for a minimum of sixty days (without service on the defendant during that time) to allow the government time to conduct its own investigation and to determine whether to join the suit.

19. Any person who violates the FCA is liable for a civil penalty of not less than $5,000, up to $11,000, for each violation, plus three times the loss sustained by the United States of America. 31 U.S.C. §3729(a).

B. The Benefits of EHR

20. EHR allow healthcare providers, such as Defendant, to record and share patient information electronically instead of on paper.

21. EHR afford health providers the capability of achieving benchmarks that can lead to improved patient care. The potential benefits of EHR involve: (i) having patients more involved in their own health care; (ii) improving the coordination of care; (iii) making health care safer and more efficient; (iv) reducing health disparities; and (v) in the end, improving health for everyone.

C. The EHR Incentive Programs

22. In light of the benefits of EHR, and to encourage more providers like Defendant to establish a system of using EHR, Medicare and Medicaid EHR incentive programs were created (the "EHR Incentive Programs"). CMS oversees the Medicare EHR incentive program and the state Medicaid agencies manage the Medicaid EHR incentive program.

23. The EHR Incentive Programs provide incentive payments for certain healthcare providers to use EHR technology in ways that can positively impact patient care.

24. To take advantage of the Medicare EHR incentive program, an eligible healthcare provider needs to adopt certified EHR technology ("CEHRT"). CEHRT means that an EHR system meets a certain minimum standard and captures and stores data in a structured way.

25. The EHR Incentive Programs offer incentive payments for eligible providers who comply with the programs, with the hope being that along with such compliance, will come benefits to patients in the form of better care.

D. The Incentive Payments

26. Medicare incentive payments to eligible providers are based on certain factors. In particular, regardless of the payment year, Medicare incentive payments are the product of: (i) an Initial Amount; (ii) the Medicare Share; and (iii) a Transition Factor applicable to the payment year.

27. Eligible providers can begin receiving Medicare incentive payments in any fiscal year (FY) from FY 2011 to FY 2015, if they successfully demonstrate "meaningful use" of CEHRT. The federal fiscal year, also known as a program year, for eligible hospitals and critical access hospitals ("CAH") in relation to the EHR Incentive Programs begins on October 1st of each year and ends on September 30th of the following year.

28. Once CEHRT has been purchased and implemented by an eligible healthcare provider, the next step towards obtaining Medicare incentive payments is to demonstrate "meaningful use."

29. Demonstrating "meaningful use" means that the provider needs to show Medicare/CMS that it is using its EHR technology to improve care in ways that can be measured.[2]

E. Incentive Payments Require Attesting to "Meaningful Use"

30. To secure Medicare incentive payments, providers must demonstrate annually that they are meaningfully using CEHRT through a process called "attestation."

31. Attestation is an electronic legal statement that providers submit through the Medicare EHR incentive program website to declare that they have met the thresholds and all of the requirements of the EHR Incentive Program.

32. As part of the attestation process, the provider must acknowledge and agree to the

[2] Said another way, to promote investment in health information technology ("HIT"), and EHR technology, legislation offers financial incentives to professionals and hospitals that achieve "meaningful use" of EHR and attest that they comply with federal regulations to protect, secure, keep private, and not disclose personally identifiable information/personal health information ("PII/PHI").

following language contained in the Attestation Disclaimer:

> I certify that the foregoing information is true, accurate, and complete. I understand that the Medicare EHR Incentive Program payment I requested will be paid from Federal funds, that by filing this attestation I am submitting a claim for Federal funds, and that the use of any false claims, statements, or documents, or the concealment of a material fact used to obtain a Medicare EHR Incentive Program payment, may be prosecuted under applicable Federal or State criminal laws and may also be subject to civil penalties.

33. To receive incentive payments under the EHR Incentive Programs, eligible hospitals must attest to the meaningful use of a certified EHR by meeting and reporting on thresholds (or stages) for a number of objectives.

34. Although not particularly relevant to the allegations here, in the EHR Incentive Programs, there are three stages (or thresholds) of "meaningful use"; each one has benchmarks that progress, like the rungs on a ladder, to help providers get closer to improving health outcomes.

35. Meaningful Use Stage 1 requirements focus on providers capturing patient data and sharing that data either with the patient or with other healthcare professionals. Meaningful Use Stage 2 requirements focus on advanced clinical processes. Meaningful Use Stage 3 requirements have not yet been finalized although CMS previously stated that it would be published in the first half of 2015 and implemented in 2016.

36. Per CMS, an eligible hospital must attest to a ninety-day consecutive period in the first year of joining the program (Stage 1). With the exception of 2014, the eligible hospital must then attest for a full program year and every year after that. In general, the attestation deadline is November 30th following the end of the current federal fiscal year.[3]

37. At each stage, a provider can demonstrate meaningful use by meeting certain criteria, like providing prescriptions electronically or recording valuable information about

[3] At times, CMS has extended the attestation deadline. For example, the attestation deadline for the full 2013 program year was extended to February 28, 2014. For the full 2015 program year, attestation has been extended so that instead of attesting on November 30, 2015, eligible hospitals must attest between January 4, 2016 and February 29, 2016.

patients, such as vital signs and smoking status.

38. Some of these meaningful use requirements put the focus on patients, and how EHR gives them better interaction with their providers or their care plan. For example, such as getting an electronic reminder for follow-up care.

39. Other meaningful use requirements focus on providers, and how EHR can help them make more informed decisions, deliver better care, or collaborate with other providers.

F. Two Attestations Particularly Relevant to the Complaint

40. Among other things, in order to obtain Medicare incentive payments, providers are required to specifically attest to: (i) the completion of an "accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate" (*see* 45 C.F.R. §164.308(a)); and (ii) the submission of clinical quality measures ("CQM") data through CEHRT for Stage 2 meaningful use.

1. Attesting to Security

41. To participate in the EHR Incentive Programs and receive an incentive payment, among other things, hospitals are required to conduct an accurate and thorough security risk analysis to meet the standards of the Health Insurance Portability and Accountability Act. The main purpose of the security risk analysis is to ensure the privacy and security of the patients' PII/PHI created or maintained by the CEHRT.

42. To obtain Medicare incentive payments, a security risk analysis needs to be performed and attested to during each reporting period.

43. Moreover, any security updates and deficiencies that are identified during the performance of the security risk analysis should be included in the provider's risk management process and implemented or corrected as dictated by that process. Furthermore, CMS rules and audit validation requires that the security risk analysis and any necessary updates be performed prior to the end of that program year.

44. As discussed in more detail below, each year, from 2011 or 2012 through the

present, Defendant falsely attested to the government that it had conducted an appropriate security risk analysis and corrected identified security deficiencies when it had not.

2. Attesting to CQM Data from CEHRT

45. The meaningful use requirements of the EHR Incentive Programs also require providers to submit CQM data from CEHRT and attest that such data was, in fact, pulled by and from the CEHRT, and not by any other means.

46. CEHRT gives assurance to purchasers and other users that an EHR system or module offers the necessary technological capability, functionality, and security to help them meet the meaningful use criteria. Certification also helps providers and patients be confident that the electronic HIT products and systems they use are secure, can maintain data confidentially, and can work with other systems to share information.

47. When selecting an EHR system, providers should be sure that they can report the CQM they will be selecting for meaningful use reporting.

48. CMS recommends that providers pick an EHR system that can report all the CQM defined in the EHR Incentive Programs, so that they have the flexibility to choose from any of the CQM.

49. Eligible professionals (EP) and eligible hospitals must report CQM results generated from their EHR system in the Medicare/CMS Registration and Attestation System located on the Medicare/CMS website.

50. The EHR Incentive Programs require that data be recorded in CEHRT to facilitate the collection and reporting of CQM.

51. One main purpose for this requirement is so that the government's health care system can continue to move towards more efficient and responsible care, tracking progress along the way.

52. Specifically, in order to capture and share patient data efficiently, providers need CEHRT that stores data in a structured format which allows patient information to be easily retrieved and transferred, and allows the provider to use the CEHRT in ways that can aid patient

care.

53. During attestation, in addition to requiring that each provider attest that the CQM results/data being submitted to the government has been produced by CEHRT, Medicare also requires each EP, hospital, and CAH, to provide an EHR Certification ID that identifies the CEHRT being used to demonstrate meaningful use.

54. As discussed in more detail below, for the years 2011 to the present, but at least from 2014 to the present, Defendant submitted false attestations to the government that its CQM results/data came from CEHRT, when in fact it did not.

V. DEFENDANT'S FCA VIOLATIONS

A. Overview of the False Attestations to Medicare and Medicaid

55. Defendant registered for the EHR Incentive Programs in 2011.

56. Consistent with the EHR Incentive Programs, Defendant made attestations to Medicare and Medicaid with regard to: (i) its performance of security risk analyses ("Security Risk Attestations"); and (ii) its data being from CEHRT ("Data Attestations").

57. Defendant accessed the Medicare attestation system and made attestations to Medicare for program years 2012 through 2014 as identified by their National Provider Identifier ("NPI") number.

58. Defendant accessed the Kansas Medicaid attestation system and made attestations to Kansas Medicaid for various undisclosed program years beginning in at least 2012 and presumably through 2014 as identified by the Kansas Department of Health and Environment.

59. Although the specific dates of Coffey's Kansas Medicaid attestations are unknown, including with respect to the specific years of attestation, according to the Kansas Department of Health and Environment, by March 2013, Coffey had received at least $286,043.22 from the Kansas Medicaid EHR incentive program.

60. All of Defendant's yearly Security Risk Attestations from 2012 through the present, and yearly Data Attestations in at least 2014 through the present, were knowingly false when submitted to the government.

61. As a result of the false Security Risk Attestations and false Data Attestations, the government paid Defendant substantial amounts of incentive payments for program years 2012 through 2014. In addition, if this wrongful conduct is not stopped, the government will continue to wrongfully pay Defendant for 2015 and future program years.

62. Defendant falsely attested that: (i) it performed essential security risk analysis commensurate with appropriate "meaningful use" standards, when, in fact it, did not; and (ii) it submitted CQM data (in 2014, at least) from its CEHRT, when, in fact, the CQM data was not from its CEHRT.

63. Thus, in violation of the FCA, Defendant knowingly submitted false claims/attestations to Medicare and Medicaid under the EHR Incentive Programs, in order to get millions of dollars of incentive payments.

64. As a result of Defendant's false attestations, Coffey improperly received, from the government, at least $3 million in meaningful use financial incentive payments and may possibly receive additional future undeserved and unadjusted incentive payments.

B. Coffey's False Security Risk Attestations

65. In June 2014, Relator Awad began working as a consultant in Coffey's IT department. Relator Awad was promoted to CIO in August of 2014.

66. By June 2014, Coffey had already made Security Risk Attestations to CMS on at least two separate occasions for the program years 2012 and 2013.

67. Shortly after Relator Awad was promoted to CIO by Coffey in August 2014, Relator Awad promptly sought to obtain copies of Coffey's most recent security risk analysis.

68. During this process, Relator Awad confirmed, on several occasions, that no security risk analysis had been performed.

69. Relator Awad learned that no security risk analyses had been performed for the years 2011 through 2013.

70. Although the CMS attestation portal noted that Coffey had attested that appropriate security risk analyses had been performed from about 2012 through 2013, Relator

Awad learned that there was no documentation, whatsoever, to support the Security Risk Attestations that would have been needed to support the meaningful use attestation to the government.

71. After learning that Coffey had never before conducted an appropriate risk analysis, in 2014, Relator Awad personally conducted some basic tests of Coffey's network security.

72. During his testing, Relator Awad quickly discovered that Coffey shared the same firewall as various Coffey county municipalities.

73. Because Coffey shared the same firewall as various Coffey county municipalities, ***anyone*** could access Coffey's private patient records simply by logging in to Coffey's website through its IP address[4] at the local schools or libraries, without any usernames or passwords.

74. Thereafter, Relator Awad arranged for a third-party company, MainNerve,[5] to perform an appropriate security risk analysis at Coffey in preparation for its upcoming meaningful use attestation to be submitted for 2014.

75. The MainNerve risk analysis was completed on or about October 16, 2014 (hereafter, the "2014 Security Risk Analysis").

76. The 2014 Security Risk Analysis identified dozens of unique vulnerabilities in Coffey's systems, including five "critical" vulnerabilities,[6] fifteen "high" vulnerabilities,[7] thirty-

---

[4] An IP address, or Internet Protocol address, is a unique string of numbers separated by periods that identifies each computer using the Internet Protocol to communicate over a network.

[5] MainNerve is a defense-grade cybersecurity firm located at 5825 Mark Dabling Boulevard, Suite 160, Colorado Springs, Colorado 80919; Telephone: (877) 362-1771. *See* MainNerve, http://mainnerve.com/about/ (last visited Dec. 26, 2015).

[6] Critical vulnerabilities "represent[] a critical risk to the infrastructure. A published exploit is likely existent resulting in a trivial attack."

[7] High vulnerabilities "include ability to gain access as root or administrative user."

four "medium" vulnerabilities,[8] and twelve "low" vulnerabilities.[9]

77. Relator Awad reported results of the 2014 Security Risk Analysis to Coffey and thereafter began attempting to address some of the highest priority vulnerabilities.

78. Coffey was not interested in devoting resources to the 2014 Security Risk Analysis findings and did not provide Relator Awad with adequate tools or support to properly address the deficiencies. Thus, despite Relator Awad's efforts, very few of the deficiencies noted in the 2014 Security Risk Analysis were corrected.

79. Soon after Coffey's failure to adopt the 2014 Security Risk Analysis, or conduct any other appropriate security risk analysis as required by law, Coffey caused another false Security Risk Attestation to be submitted in 2014, to the government, seeking incentive payments under the EHR Incentive Programs.

80. Relator Awad refused to support the 2014 attestations by Coffey, and was terminated while attempting to correct the numerous security deficiencies identified by MainNerve.

81. Relators believe that, to the present date, Coffey is continuing to seek Medicare and Medicaid incentive payments by falsely attesting to security risk analyses, despite refusing to perform security updates as necessary and refusing to correct numerous known security deficiencies.

C. Coffey's False Data Attestations

82. Sometime around November 2014, Coffey accessed the Medicare attestation system to apply for EHR incentive payment from the government for the full 2014 program year. During this process, Coffey attested that the CQM file data was electronically generated, as required by law.

---

[8] Medium vulnerabilities "that provide limited exploit of read and write capabilities, directory browsing and/or Denial of Service (DoS) attacks."

[9] Low vulnerabilities that "enable the enumeration of information about the system without requiring user authentication (such as open ports)."

83. However, this attestation by Coffey was knowingly false when made because Coffey knew that certain CQM data was not electronically generated, but was in fact manually generated with the intention of misleading CMS.

84. Although Coffey was required to attest that the CQM data submitted was from a CEHRT, instead, the Company manually created the data and attempted to make it appear as if it was generated electronically via the CEHRT system.

85. Again, Relator Awad refused to support the 2014 attestations by Coffey.

86. The Company nonetheless submitted the knowingly false 2014 attestations on or about April 27, 2015, with the government.

87. Relator Awad's employment with Coffey ended around July 2015.

VI. DAMAGES CAUSED BY DEFENDANT'S FALSE CLAIMS

88. In compliance with the Health Information Technology for Economic and Clinical Health Act's requirement, CMS has posted the names, business phone numbers, and business addresses of Medicare EP, eligible hospitals, and CAH that have successfully demonstrated meaningful use and received incentive payments.

89. According to CMS's list of eligible hospital recipients of Medicare and Medicaid EHR Incentive Programs payments as of June 2015, Coffey has received $1,202,600, $961,968, and $623,280 for program years 2012, 2013, and 2014, respectively, in incentive payments.

90. According to the Kansas Department of Health and Environment as of March, 2013, Coffey received $286,043.22 in Kansas Medicaid incentive payments.

91. Because Coffey's attestations from at least 2012 through 2014 were knowingly false when submitted to the government, Coffey improperly and wrongfully received from the government, at least $3 million of EHR incentive payments.

92. It is Relators' belief that Coffey's false attestation practices continue through the present.

93. Furthermore, per CMS rules and regulations, beginning with the 2015 program year, failure to implement and demonstrate meaningful use under the EHR Incentive Programs is

supposed to result in a decreased payment. Provided that Coffey continues to submit false attestations in violation of the EHR Incentive Programs, it is highly likely that Coffey will not receive an adjusted payment but will instead wrongfully receive the full EHR incentive payments.

VII. COUNT I—FCA 31 U.S.C. §3729(a)(1)(A)

94. Relators incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

95. This is a claim for treble damages and penalties under the FCA, 31 U.S.C. §§3729, *et seq*., as amended.

96. By virtue of the acts set forth above, Defendant presented or caused to be presented, false or fraudulent claims for payment or approval to the government in violation of 31 U.S.C. §3729(a)(1).

97. The United States of America, unaware of the falsity of the claims, paid and continues to pay claims that would not be paid but for Defendant's unlawful conduct.

98. As a result of the Defendant's acts, the United States of America has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

VIII. COUNT II—FCA 31 U.S.C. §3729(a)(1)(B)

99. Relators incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

100. This is a claim for treble damages and penalties under the FCA, 31 U.S.C. §§3729, *et seq*., as amended.

101. By virtue of the acts set forth above, Defendant has knowingly made, used, or caused to be made or used, false or fraudulent records and statements, and omitted material facts, to get false and fraudulent claims paid or approved, within the meaning of 31 U.S.C. §3729(a)(1)(B).

102. The United States of America, unaware of the falsity of the records, statements, and claims made or caused to be made by the Defendant, paid and continues to pay claims that

would not be paid but for Defendant's unlawful conduct.

103. As a result of the Defendant's acts, the United States of America has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

IX. PRAYER FOR RELIEF

WHEREFORE, Relators, on behalf of the United States of America, respectfully request this Court to enter judgment for Relators, and on behalf of the United States, and against Defendant, on each Count of this Complaint, and to impose judgment against the Defendant and in favor of Relators, on behalf of the United States, as follows:

(a) for the United States of America to be awarded damages in an amount equal to three times the loss sustained by the United States because of false claims and fraud alleged herein, as the FCA provides;

(b) for civil penalties of statutorily-determined amounts for each and every false claim that Defendant presented to the United States of America and/or its representatives;

(c) for an award to Relators for reasonable expenses, attorneys' fees, and costs incurred in connection with this action;

(d) for Relators to be awarded the maximum amount allowed, pursuant to the FCA; and

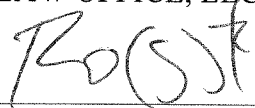
(e) that this Court award such other and further relief as it deems proper.

X. DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Relators hereby demand a trial by jury and designate Kansas City as the place for trial.

Dated: January 15, 2016

STEWART LAW OFFICE, LLC



ROSS HENRY STEWART (Bar # 26063)

9270 Glenwood, Suite C
Overland Park, KS 66212
Telephone: (816) 237-8395
E-mail: RossHenryStewart@gmail.com

ROBBINS ARROYO LLP
KEVIN A. SEELY
600 B Street, Suite 1900
San Diego, CA 92101
Telephone: (619) 525-3990
Facsimile: (619) 525-3991
E-mail: kseely@robbinarroyo.com

Attorneys for Qui Tam Plaintiffs

1041263