ROBBINS UMEDA LLP
BRIAN J. ROBBINS (190264)
KEVIN A. SEELY (199982)
GREGORY E. DEL GAIZO (247319)
600 B Street, Suite 1900
San Diego, CA 92101
Telephone: (619) 525-3990
Facsimile: (619) 525-3991

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
THOMAS J. O'REARDON II (247952)
600 B Street, Suite 1550
San Diego, CA 92101
Telephone: (619) 338-1100
Facsimile: (619) 338-1101

Attorneys for Plaintiff

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF SAN DIEGO

MARK LOSACK, on Behalf of Himself and All Others Similarly Situated, Plaintiff, v. SAIC INC., a Delaware corporation, Defendant.	Case No. **37-2011-00102318-CU-MT-CTL** CLASS ACTION COMPLAINT DEMAND FOR JURY TRIAL

Plaintiff Mark Losack ("Plaintiff") brings this action on behalf of himself and all others similarly situated against defendant SAIC, Inc. ("SAIC" or "Defendant"), and states:

NATURE OF THE ACTION

1. This is a consumer class action lawsuit on behalf of all similarly situated persons in California concerning the loss of personally identifiable and protected health information ("PII/PHI") for 4.9 million military service members, retirees, and their families who received health care through TRICARE.

2. Defendant SAIC is a government contractor supporting the Military Health System. SAIC's responsibilities include securing and safely transporting computer backup tapes containing the PII/PHI for TRICARE beneficiaries. According to SAIC, on or about September 14, 2011, computer backup tapes containing confidential personally identifiable and protected health information were stolen from the vehicle of the SAIC employee charged with transporting the backup tapes from one federal facility to another. The compromised PII/PHI data, which dated back to 1992, included Plaintiff and Class (as defined herein) members' social security numbers, addresses, telephone numbers, diagnoses, treatment information, provider names, provider locations, clinical notes, lab test results, prescription information, and other patient information.

3. This security breach occurred because SAIC failed to adequately safeguard the PII/PHI. SAIC could have transmitted the computer backup data by secure electronic means rather than physical transportation, or transferred the information by more responsible means. This is not the first time SAIC lost sensitive data entrusted to it. At least six prior instances have been documented. Just last year, SAIC allowed another theft of computer backup tapes containing sensitive confidential information.

4. Pursuant to a contract with TRICARE, SAIC is obligated to transport computer backup tapes containing the personal information of TRICARE members from one federal facility to another. Without adequate training, supervision, or procedures, SAIC had a single employee using his own vehicle for this task. The SAIC employee put the backup tapes in his car, and then parked the car on a public street in San Antonio, Texas for the entire day. The

tapes were then taken from the car. The data was not properly encrypted according to appropriate standards. Therefore, because of SAIC's actions and omissions, unauthorized third parties are able to access the private, personal data of an estimated 4.9 million people.

5. SAIC was aware of this security breach but withheld information about and failed to timely notify Plaintiff and other Class members of the unauthorized third-party access to their PII/PHI. Though the theft occurred on September 14, 2011, SAIC's first notice to Plaintiff and Class members of the security breach was by letter dated November 11, 2011. On information and belief, there are additional persons affected by the theft that SAIC still has yet to notify. This violates California Civil Code sections 1798.29 and 1798.82, which requires prompt notice of any such security breach.

6. Because of SAIC's actions and omissions, millions of TRICARE beneficiaries have had their PII/PHI compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identity theft, and have otherwise suffered losses as set forth herein

7. Plaintiff brings this action on behalf of himself and other similarly situated consumers in California who subscribed to TRICARE, and whose PII/PHI was entrusted to SAIC and compromised as a result of the events surrounding the data theft on September 14, 2011. Plaintiff alleges violations of the Security Requirements for Consumer Records, Civil Code sections 1798.29 and 1798.80, *et seq.*, and the common law as a result of SAIC's misconduct.

JURISDICTION AND VENUE

8. This Court has jurisdiction pursuant to Code of Civil Procedure section 410.10 and Article VI, section 10 of the California Constitution, because this case is not a cause given by statute to other trial courts.

9. Venue is proper in this Court in that many of the acts and transactions giving rise to this action occurred in this County and because Defendant:

(a) is authorized to conduct business in this County and has intentionally availed itself of the laws and markets within this County;

(b) does substantial business in this County; and

(c) is subject to personal jurisdiction in this County.

PARTIES

10. Plaintiff is a citizen of the state of California and resides in San Diego, California. He is a retired Marine Colonel. Plaintiff is a participant in TRICARE. TRICARE possesses Plaintiff's sensitive personal and medical information. On November 11, 2011, Plaintiff received a letter from SAIC alerting him that his highly confidential personal information was stolen from SAIC in the manner described herein.

11. Defendant SAIC (also known as Science Applications International Corporation) is a Delaware corporation with its executive offices located at 1710 SAIC Drive, McLean, Virginia. Until 2009, SAIC was headquartered in San Diego, California, and still has a major presence there. SAIC is a provider of scientific, engineering, systems integration, and technical services and solutions in the areas of defense, health, energy, infrastructure, intelligence, surveillance, reconnaissance, and cybersecurity to all agencies of the U.S. Department of Defense ("DoD"), the intelligence community, the U.S. Department of Homeland Security and other U.S. Government civil agencies, state and local government agencies, foreign governments, and customers in select commercial markets. SAIC is a prime contractor to the DoD to provide information technology services and electronic health record systems support to the TRICARE Management Activity ("TMA") Military Health System, which manages the TRICARE healthcare program for more than nine million active duty, National Guard and Reserve, retired service members, and their families and beneficiaries.

FACTUAL ALLEGATIONS

TRICARE and SAIC

12. TRICARE, formerly known as the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS), is a health care program of the DoD Military Health System. It provides civilian health benefits for military personnel, military retirees, and their dependents, including some members of the reserve component. The TRICARE program is managed by TMA under the authority of the Assistant Secretary of Defense (Health Affairs). TRICARE

provides medical and health services, pharmacy benefits, dental options, and other special programs to its participants.

13. TRICARE contracted with SAIC to transfer, store, secure, and protect the private information of certain TRICARE participants, including Plaintiff and the Class members. As a government contractor, SAIC had a duty to ensure the privacy of TRICARE member's confidential information.

SAIC's History of Improperly Handling Private Data

14. The September 2011 security breach was not the first time SAIC failed to properly secure data. A bipartisan congressional letter dated December 2, 2011, to Dr. Jonathan Woodson, the Director of TRICARE and the Assistant Secretary of Defendant for Health Affairs, identified "at least six prior security incidents [involving SAIC] due to malware infections, stolen computers, and, last year, stolen computer backup tapes."[1]

15. For example, on January 12, 2005, thieves broke into a SAIC facility in San Diego, California, and stole a computer containing the personal information of present and past stockholders of Defendant. This personal information included social security numbers, addresses, telephone numbers, and records of financial transactions.

16. On July 20, 2007, the SAIC announced that it improperly transferred unencrypted, private health information of approximately 867,000 U.S. service members and their families across the internet through an unsecure server. The wrongfully transmitted information included names, addresses, social security numbers, birth dates, and other health information. Though it waited until July 2007 to announce the issue, Defendant knew about the problem since May of that year.

17. On June 30, 2010, SAIC notified the Maryland Office of the Attorney General that it had discovered a "theft of backup tapes" that may have exposed personal information including names, social security numbers, and birth dates.

[1] *See* http://markey.house.gov/docs/2011_1202_letter_to_director_of_tricare.pdf (last visited December 7, 2011).

18. Despite numerous complaints from federal officials about SAIC's mishandling of confidential data, SAIC has received approximately $20 billion in federal contracts over the last three years.

The Theft of Plaintiff and Class Member's Personal Confidential Data

19. On September 28, 2011, TRICARE announced that on September 14, 2011, an unknown person stole backup data tapes from an SAIC employee's car containing the confidential PII/PHI data of approximately 4.9 million military clinic and hospital patients.

20. The computer backup tapes were stolen from the SAIC employee's 2003 Honda Civic, which was parked on a downtown street in San Antonio, Texas, and left unattended from approximately 8:00 a.m. until 4:30 p.m. on the date of the theft. The SAIC employee had possession of the computer tapes because he was purportedly transporting them from one government facility to another. SAIC describes this method of transporting these backup tapes as "routine procedure" for the company.

21. The information on these computer backup tapes contained Plaintiff's and the Class members' sensitive PII/PHI, including their social security numbers, addresses, telephone numbers, diagnoses, treatment information, provider names, provider locations, clinical notes, lab test results, prescription information, and other patient information.

22. Only a portion of the confidential PII/PHI on the computer backup tapes was encrypted.

23. Though TRICARE announced the theft on September 28, 2011, Plaintiff was not notified that his PII/PHI was stolen until receiving a letter dated November 11, 2011. On information and belief, SAIC knew on September 14, 2011, or soon thereafter, that Plaintiff's personal information was on the stolen computer backup tapes. Further, on information and belief, SAIC still has not notified all individuals that had their personal PII/PHI stolen.

24. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction, Plaintiff's and the Class member's confidential PII/PHI was stolen and disseminated into the public domain without their knowledge, authorization, and/or consent and, as a further direct and/or proximate result, suffered, and will continue to suffer, damages including, without

limitation, expenses for credit monitoring and insurance, out of pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

CLASS ACTION ALLEGATIONS

25. Plaintiff seeks certification of a Class consisting of:

> All persons within California who subscribed to TRICARE, and whose PII/PHI was compromised as a result of the events surrounding the data theft on September 14, 2011.

Excluded from the Class is SAIC and any of its officers, directors, and employees.

26. ***Numerosity***. The members of the Class are so numerous that their individual joinder is impracticable. Plaintiff is informed and believes, and on that basis alleges, that the proposed Class contains hundreds of thousands of members. The precise number of Class members is unknown to Plaintiff. The true number of Class members is known by the Defendant, however, and thus, may be notified of the pendency of this action by first class mail, electronic mail, and by published notice.

27. ***Existence and Predominance of Common Questions of Law and Fact.*** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual Class members. These common legal and factual questions include, but are not limited to, the following:

(a) whether Defendant violated California Civil Code sections 1798.29 and 1798.80;

(b) whether Defendant willfully, recklessly, and/or negligently failed to maintain reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class members' private information;

(c) whether Defendant was negligent in storing and transporting Plaintiff's and the Class members' private information;

(d) whether Defendant owed a duty to Plaintiff and the Class members to exercise reasonable care in protecting and securing their private information;

(e) whether Defendant breached its duty to exercise reasonable care in protecting and securing Plaintiff's and the Class members' private information;

(f) whether Defendant was negligent in failing to keep Plaintiff's and the Class members' private information secure;

(g) whether by publicly disclosing Plaintiff's and the Class members' private information without authorization, Defendant invaded Plaintiff's and the Class members' privacy;

(h) whether Plaintiff and the Class members sustained damages as a result of Defendant's failure to secure and protect their private information; and

(i) whether Defendant's conduct complained of herein was intentional and knowing.

28. ***Typicality***. Plaintiff's claims are typical of the claims of the members of the Class in that he is a member of the Class he seeks to represent.

29. ***Adequacy of Representation***. Plaintiff will fairly and adequately protect the interests of the members of the Class. Plaintiff has retained counsel highly experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously. Plaintiff has no adverse or antagonistic interests to those of the Class.

30. ***Superiority***. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The potential recovery available to individual Class members is relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against the Defendant. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. Further, the adjudication of this action presents no unusual management difficulties.

31. Adequate notice can be given to Class members directly using information maintained in Defendant's records or through notice by publication.

FIRST CAUSE OF ACTON

Violation of Security Requirements for Consumer Records, Civil Code Sections 1798.29 and 1798.80, *et seq.*

32. Plaintiff realleges and incorporates the preceding paragraphs as if set forth fully herein.

33. California law requires any business that retains personal information from its customers (including financial or personal identification data) to implement and maintain reasonable security procedures and practices to protect such information from unauthorized access, destruction, use, modification, or disclosure.

34. California Civil Code sections 1798.29 and 1798.82 further require that any business that retains personal information from its customers (including personal identification data) must promptly and "in the most expedient time possible and without unreasonable delay" disclose any breach of the security of the system containing such retained data.

35. Defendant failed to implement and maintain reasonable security systems, including its failure to properly encrypt data and failure to transfer data in a secured manner.

36. Defendant also unreasonably delayed and failed to disclose to Plaintiff and the Class, in the most expedient time possible and without unreasonable delay, the breach in security of non-public information of Plaintiff and the Class when Defendant knew or reasonably believed such information had been acquired by an unauthorized person or persons.

37. On information and belief, no law enforcement agency determined or instructed Defendant herein that notification of Plaintiff or the Class members would impede a criminal investigation.

38. Defendant also failed to comply with the privacy notification rights required in California Civil Code section 1798.83.

39. As a direct and proximate result of Defendant's acts and omissions described herein, Plaintiff and the Class have suffered damages, including, but not limited to, loss of and invasion of privacy, loss of property, loss of money, loss of control of their personal non-public information, fear and apprehension of fraud and loss of money and control over their personal

financial and other non-public information, and the burden of monitoring their financial and credit accounts, and taking other actions to protect themselves from fraud or potential fraud, monetary loss, and injury to their credit and finances. The amount of such damages will be proven at trial, but is in excess of the minimum jurisdiction of this Court.

SECOND CAUSE OF ACTION

Negligence

40. Plaintiff realleges and incorporates the preceding paragraphs as if set forth fully herein.

41. Defendant had a duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' confidential information.

42. Defendant violated its duty by failing to exercise reasonable care and safeguard and protect Plaintiff's and the Class members' confidential information.

43. It was reasonably foreseeable that Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' confidential information would result in an unauthorized third-party gaining access to such information for no lawful purpose.

44. Plaintiff and the Class members were damaged as a direct and/or proximate result of Defendant's failure to secure and protect their confidential information in the form of, without limitation, expenses for credit monitoring and insurance, out of pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm—for which they are entitled to compensation.

45. Defendant's wrongful actions and/or inaction, as described above, constitute negligence at common law.

THIRD CAUSE OF ACTION

Invasion of Privacy by Public Disclosure of Private Facts

46. Plaintiff realleges and incorporates the preceding paragraphs as if set forth fully herein.

47. Defendant's failure to secure and protect Plaintiff's and the Class members' confidential information directly resulted in the public disclosure of such private information.

48. Plaintiff's and the Class members' confidential information is not of a legitimate public concern; its publicity would be, is and continues to be, offensive to reasonable people.

49. Plaintiff and the Class Members were damaged as a direct and/or proximate result of Defendant's invasion of their privacy by publicly disclosing their private information in the form of, without limitation, expenses for credit monitoring and insurance, out of pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm—for which they are entitled to compensation.

50. Defendant's wrongful actions and/or inaction, as described above, constitute an invasion of Plaintiff's and the Class members' privacy by publicly disclosing their private facts.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief in interim orders and by way of entry of final judgment in his favor, in favor of those he seeks to represent, and against Defendant:

A. On all causes of action, an order certifying this case as a class action and appointing Plaintiff and his counsel to represent the Class;

B. Awarding declaratory and injunctive relief as permitted by law or equity, including: enjoining Defendant from continuing the unlawful practices as set forth herein, and directing Defendant to notify, with Court supervision, victims of their conduct and requiring Defendant to pay for Plaintiff and the Class members': (i) credit monitoring; (ii) identity theft insurance; and (iii) requiring Defendant to submit to periodic compliance audits by a third party regarding the security of consumers' private information in its possession, custody, and control;

C. Awarding Plaintiff and members of the Class actual damages in an amount according to proof under all causes of action herein entitling Plaintiff and members of the Class to actual damages;

D. Awarding Plaintiff and members of the Class exemplary damages for Defendant's knowing, willful, and intentional conduct, as alleged herein;

E. Awarding Plaintiff and members of the Class pre-judgment and post-judgment interest, as well as their reasonable attorneys' and expert-witness fees, and other costs; and

F. For such additional or further relief as the Court finds just and appropriate.

JURY DEMAND

Plaintiff demands a trial by jury of all issues which are subject to adjudication by a trier of fact.

DATED: December 9, 2011

ROBBINS UMEDA LLP
BRIAN J. ROBBINS
KEVIN A. SEELY
GREGORY E. DEL GAIZO

Brian J. Robbins /w permission CBS
BRIAN J. ROBBINS

600 B Street, Suite 1900
San Diego, CA 92101
Telephone: (619) 525-3990
Facsimile: (619) 525-3991

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD
THOMAS J. O'REARDON II
600 B Street, Suite 1550
San Diego, CA 92101
Telephone: (619) 338-1100
Facsimile: (619) 338-1101

Attorneys for Plaintiff

678037