UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA

VIRGINIA E. GAFFNEY, et al. Plaintiffs, vs. TRICARE MANAGEMENT ACTIVITY, et al. Defendants.	Case No. 1:11-cv-01800-RLW
VON W. RICHARDSON, et al. Plaintiffs, vs. TRICARE MANAGEMENT ACTIVITY, et al Defendants.	Case No. 1:11-cv-01961-RLW
JAMES F. BIGGERMAN, JR. Plaintiff, vs. TRICARE MANAGEMENT ACTIVITY, et al Defendants.	Case No. 1:11-cv-02142-RLW
MURRY MOSKOWITZ, et al. Plaintiff, vs. TRICARE MANAGEMENT ACTIVITY, et al Defendants.	Case No. 1:11-cv-02283-RLW
JESSICA PALMER, et al. Plaintiff, vs. TRICARE MANAGEMENT ACTIVITY, et al Defendants.	Case No. 1:12-cv-00008-RLW

CONSOLIDATED REPLY BRIEF IN SUPPORT OF MOTION FOR ENTRY OF ORDER: (1) CONSOLIDATING RELATED ACTIONS, and (2) APPOINTING PLAINTIFFS' INTERIM CO-LEAD COUNSEL

Pursuant to Rules 42(a) and 23(g) of the Federal Rules of Civil Procedure, Plaintiffs in the Related Actions jointly submit this consolidated reply in support of their Motion for Entry of Order: (1) Consolidating Related Actions and (2) Appointing Plaintiffs' Interim Co-Lead Counsel.[1]

This Court should grant consolidation because all Defendants *agree* to consolidation if Plaintiffs file a consolidated amended complaint – which Plaintiffs have attached hereto as Exhibit A. *See* Defendant Science Applications International Corporation's ("SAIC") Response to Plaintiffs' Motion to Consolidate And Motion to Appoint Interim Co-Lead Counsel of Putative Class ("SAIC's Motion") at 1; see also Defendants' Opposition to Plaintiffs' Motion For An Entry Of An Order For Consolidation And Appointment of Co-Class Counsel ("Government's Motion") at 1. Even without that consolidated amended complaint, the Court should consolidate the Related Actions because the Government Defendants concede there is overlap in the Related Actions and they do not dispute that the Related Actions all arise from the same incident. Given that the Related Actions involve common questions of law and fact, consolidation is appropriate.

This Court should also grant the appointment of interim co-lead counsel because all Plaintiffs in the Related Actions have agreed to the appointment of the proposed counsel to protect the interests of the putative class and to promote the orderly and efficient prosecution of

[1] The "Related Actions" are (1) *Gaffney, et al. v. TRICARE, et al.*, No. 1:11-cv-01800-RLW; (2) *Richardson, et al. v. TRICARE, et al.*, No. 1:11-cv-01961-RLW; (3) *Biggerman, et al. v. TRICARE, et al.*, No. 1:11-cv-02142-RLW; (4) *Moskowitz, et al. v. TRICARE, et al.*, No. 1:11-cv-02283-RLW; and (5) *Palmer, et al. v. TRICARE, et al.*, No. 1:12-cv-00008-RLW.

this litigation. Defendants have no real stake in that decision. The Court should disregard Defendants' objection to the Plaintiffs' proposal based on arguments as to the *merits* of a motion not yet filed against the proposed consolidated amended complaint filed hereto and arguments as to the viability of a class motion not yet before this Court. Plaintiffs' proposal is more efficient and orderly.

I. The Related Actions Should be Consolidated.

The Government Defendants concede there is overlap among the Related Actions and do not dispute that the Related Actions all arise from their failure to properly safeguard, and public disclosure of, the private medical and other personal information of more than 4.9 million current and former military personnel and their families. The Government Defendants nevertheless argue that consolidation is improper because there are some variations in the claims and parties in the underlying complaints in the Related Actions. The goal of consolidation here, however, is to prosecute one consolidated action rather than the five separate cases currently before the Court. Indeed, Government Defendants' argument fails now that Plaintiffs have submitted their proposed consolidated amended complaint, attached hereto as Exhibit A.

In any event, courts routinely consolidate cases with variations in claims and parties as long as the cases involve a common question of law or fact. *See, e.g., Colbert v. F.B.I.*, 275 F.R.D. 30, 32 (D.D.C. 2011) ("Although these cases have been commenced against different defendants, because all three cases stem from similar allegations . . . these cases contain common questions of law or fact. Consolidation would thus facilitate a more efficient resolution of these cases."); *Nat'l Ass'n of Mortgage Brokers v. Bd. of Governors of the Fed. Reserve Sys.*, 770 F. Supp. 2d 283, 287 (D.D.C. 2011) ("cases may be consolidated even where certain defendants are

named in only one of the Complaints"); *Hanson v. Dist. of Columbia*, 257 F.R.D. 19, 21–22 (D.D.C. 2009) (consolidating cases with overlapping and differing claims).

The Related Actions involve numerous common questions of law or fact including, among other things, the Government Defendants' liability and responsibility to Tricare members under the Federal Privacy Act for their failure to safeguard, and their public disclosure of, private medical and other personal information.

The Government Defendants also ignore common sense in arguing that this Court should deny consolidation because it must conduct an individualized review of each plaintiff's claim of injury to determine if each plaintiff has standing. Each named plaintiff in the consolidated amended complaint can have his or her standing challenged at the appropriate time; to wit a 12(b)(1) motion filed against the consolidated complaint.

Contrary to the Government Defendants, SAIC argues, and Plaintiffs agree, that issues such as standing and class certification are common issues that warrant consolidation. But in making this argument SAIC improperly and prematurely delves into the merits of the Plaintiffs' claims and the propriety of a class certification motion not yet before this Court. Plaintiffs decline Defendants' invitation to prematurely address these issues, but simply note that numerous courts, including this court, have denied motions to dismiss data security breach claims in similar cases.[2]

[2] *See, e.g., In re Dep't of Veterans Affairs (VA) Data Theft Litig.*, Misc. Action No. 06-0506 (JR), MDL No. 1796, 2007 WL 7621261, at *3 (D.D.C. Nov. 16, 2007) (denying in part defendants' motion to dismiss under 12(b)(1), (5), and (6) because "[t]he named plaintiffs in this case allege emotional and pecuniary harm by the theft of the hard drive containing their personal information."); *Kvech v. Holder*, No. 10-CV-545 RLW, 2011 WL 4369452 (D.D.C. Sept. 19, 2011) (denying motion to dismiss); *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011) (reversing district court's dismissal of negligence and implied contract claims for damages based on card replacement costs and credit insurance); *In re Michaels Stores Pin Pad Litig.*,

In any event, all Defendants concede that consolidation is proper if the Plaintiffs intend to pursue identical claims in a new consolidated amended complaint. That is precisely what Plaintiffs are in the process of doing – they have prepared a consolidated amended complaint (attached hereto as Exhibit A) which will be filed upon the entry of the proposed order consolidating the actions – and thus, by Defendants' own concession, consolidation is proper.[3]

II. This Court Should Appoint Interim Co-Lead Counsel

Defendants' attack on Plaintiffs' proposed leadership structure deserves little credence:

> [I]t is often the defendants, preferring not to be successfully sued by anyone, who supposedly undertakes to assist the court . . . it is a bit like permitting a fox, although with a pious countenance, to take charge of the chicken house.

Eggleston v. Chicago Journeymen Plumbers Local Union No. 130 U.A., 657 F.2d 890, 895 (7th Cir. 1981); *see also In re Baan Co. Sec. Litig.*, 186 F.R.D. 214, 234 n.1 (D.D.C. 1999) (in PLSRA cases "[d]efendants generally have been held to lack standing to challenge the appointment of lead plaintiff.") (citing authorities). Because the appointment of interim counsel to protect the interests of the Plaintiffs and putative class is an issue that is uniquely addressed to only the Plaintiffs and the putative class and because Defendants do not have a genuine stake in the selection of lead counsel, the cases cited by Defendants regarding the need to confer with them do not apply. Notably, those decisions involve discovery disputes that *are* well-suited for resolution under Local Rule 7(m), not the arrangements by which Plaintiffs' counsel intend to

---

___F.Supp.2d___, No. 11 C 3350, 2011 WL 5878373, at *6 (N.D. Ill. Nov. 23, 2011) (denying in part motion to dismiss).

[3] Defendants also complain that Plaintiffs should dismiss all other complaints as moot and non-operative under Rule 41. As Plaintiffs explained in their consolidation brief, Rule 41 dismissals are not (a) a prerequisite to consolidation under the Federal Rules, this District's local rules, or this Court's individual rules, (b) supported by majority precedent in this or any other jurisdiction, or (c) warranted to promote the efficient and effective management of this or any other consolidated class action litigation. Indeed, Defendants cite no authority for this argument. Therefore, Plaintiffs respectfully request that the Court disregard this partial (and mostly moot) opposition and grant consolidation of the Related Actions.

prosecute the case against Defendants. Thus, the request for appointment of interim counsel should not be denied on this basis.

The Government Defendants also ask this Court to ignore the plain language and intent of Rule 23(g) and wait until class certification is granted to appoint class counsel. However, Federal Rule of Civil Procedure 23(g)(3) explicitly states that "[t]he court may designate interim counsel . . . *before* determining whether to certify the action as a class action." (emphasis added). *See also* Advisory Committee Note to 23(g)(2)(A)[4] ("authorizes the court to designate *interim* counsel during the *pre-certification* period if necessary to protect the interests of the putative class.") Fed. R. Civ. P. 23(g)(2)(A) advisory committee note (emphasis added). "[D]esignation of interim counsel clarifies responsibility for protecting the interests of the class during precertification activities, such as making and responding to motions, conducting any necessary discovery, moving for class certification and negotiating settlement." *See* Manual for Complex Litigation, Fourth, § 21.11, at 246 (Federal Judicial Center 2004). Therefore, under Rule 23(g)(2)(A), appointment of interim co-lead counsel will best promote the protection of the putative class and promote the effective and efficient prosecution of this litigation.

SAIC wrongly claims that the Plaintiffs have not alleged any interests of the putative class that will go unprotected if interim counsel is not appointed, but as articulated by the advisory committee notes to the Federal Rules and in *Hannaford*, there are numerous interests that interim counsel protect including "presid[ing] over the articulation of the consolidated amended complaint; resist[ing] the promised motion to dismiss; and then if the matter survives in whole or in part, perform[ing] discovery and argu[ing] the motion for class certification." *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 252 F.R.D. 66, 68 (D. Me. 2008); *see*

[4] Fed. R. Civ. P. 23(g)(2)(A) was revised to become what is now Fed. R. Civ. P. 23(g)(3).

also Fed. R. Civ. P. 23(g)(2)(A) advisory committee note. SAIC also seems to concede that the appointment of interim counsel would be appropriate once a consolidated amended complaint is filed, and such a complaint is attached hereto.

SAIC also notes that two other cases against SAIC, but not the Government Defendants, are pending in other districts, and therefore, this Court should not appoint interim class counsel, or alternatively, delete the provisions in the proposed order regarding new or transferred cases. Yet, SAIC has not indicated that it seeks transfer of those cases to this Court, and thus the argument has no context other than speculation. In fact, if SAIC seeks such a transfer, it will take time that Plaintiffs cannot afford to waste. While SAIC decides whether or not to transfer those cases to this Court, Plaintiffs are still responsible for prosecuting this case and this Court will be best served by having the five Related Actions proceed in an orderly and efficient manner against both SAIC and the Government Defendants. The appointment of interim counsel will aid in the timely and efficient prosecution of these matters. *See Hannaford*, 252 F.R.D. at 68.

As authority to oppose the appointment of interim co-lead counsel, SAIC does not cite to a case, but rather a *brief* filed by a defendant in opposition to the appointment of interim counsel. *See Berniard v. Cox Commc'ns New Orleans, Inc.*, No. 209CV02996, 2009 WL 1240469 (E.D. La. Mar. 24, 2009). It is axiomatic that briefs have no precedential value. The one *decision* that SAIC cites is not binding and also distinguishable. *See Nutz for Candy v. Ganz, Inc.*, No. C 08-2873 JSW, 2008 U.S. Dist. LEXIS 79340 (N.D. Cal. Sept. 19, 2008). In *Nutz*, the Court "ha[d] a single action and a single firm seeking to be appointed interim lead counsel" when the Judicial Panel on Multidistrict Litigation was *also* considering where to transfer the cases pending in other courts. *Id.* at *4. In contrast, this case involves the private ordering of five different lawsuits that constitute all Related Actions pending in this Court and there is no indication that

the two cases against only SAIC pending in other courts will be transferred to this Court. Candidly, it is unfair to the administration of this Court and the litigation for Plaintiffs and the Court to await a decision by SAIC about whether to transfer the cases. The Plaintiffs here are ready, willing, and able to advance the litigation, and parties not before the Court should have no bearing on this Court's appointment of interim lead counsel.

Finally, Defendants complain that the motion for appointment of interim co-lead counsel should be denied because they claim only one law firm should be appointed and not the three law firms that the Plaintiffs have agreed to appoint. Plaintiffs and their counsel entered into this arrangement by consensus in order to eliminate the need for the Court to engage in decision-making with respect to this issue. Of course, the appointment of interim counsel is within the Court's discretion, and Plaintiffs appreciate that the Court may wish to approach these arrangements in a different manner. But as explained in Plaintiffs' opening brief, each proposed co-lead counsel brings unique experiences and qualifications to the table, and with the appointment of these three law firms, counsel from each of the five Related Actions is represented. Further, as discussed in the consolidation motion, co-lead counsel are dedicated to eliminate any duplication of effort by counsel and to create numerous other efficiencies for both the parties and the Court. To this end, internal groups have been formed to address the various tasks that need to be accomplished (i.e., consolidated complaint, discovery, experts, briefing, etc.) and ensure that efforts are not duplicated. Therefore, Plaintiffs respectfully request that the Court appoint Plaintiffs' proposed interim co-lead counsel.

III. Conclusion

Plaintiffs in the Related Actions respectfully request that the Court grant their Motion for Entry of Order: (1) Consolidating the Related Actions, and (2) Appointing Plaintiffs' Interim Co-Lead Counsel, and for all other just and proper relief.

Dated: February 21, 2012

Respectfully Submitted,

/s/ Tracy D. Rezvani
Tracy D. Rezvani, #464293
Mila Bartos, #464277
Rosalee B. C. Thomas, #492771
FINKELSTEIN THOMPSON LLP
1077 30th Street, N.W.
Suite 150
Washington, D.C. 20007
Telephone: (202) 337-8000
Fax: (202) 337-8090
trezvani@finkelsteinthompson.com
mbartos@finkelsteinthompson.com
rbcthomas@finkelsteinthompson.com

/s/ Stefanie M. Ramirez
Andrew N. Friedman, #375595
Agnieszka Fryszman, #459208
Stefanie M. Ramirez, #1000989
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue NW
Suite 500 West
Washington, DC 20005
Telephone: (202) 408-4600
Fax: (202) 408-4699
afriedman@cohenmilstein.com
afryszman@cohenmilstein.com
sramirez@cohenmilstein.com

/s/ Jeffrey I. Carton
James R. Denlea
Jeffrey I. Carton
Jeremiah Frei-Pearson
MEISELMAN, DENLEA, PACKMAN, CARTON & EBERZ, P.C.
1311 Mamaroneck Avenue
White Plains, NY 10605
Telephone: (914) 517-5000
Facsimile: (914) 517-5055
jdenlea@mdpcelaw.com
jcarton@mdpcelaw.com
jfrei-pearson@mdpcelaw.com

Proposed Co-Lead Counsel

EXHIBIT A

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

VIRGINIA E. GAFFNEY
4 Channel Lane
Hampton, VA 23664

JESSICA PALMER
3102 Sonora Mesa
San Antonio, Texas 78232

H.P., by her stepmother and legal guardian, Jessica Palmer

C.P., by her mother and legal guardian, Jessica Palmer

C.P. III, by his mother and legal guardian, Jessica Palmer

SHANNA HARTMAN
1926 Pelorus Avenue
Seal Beach, CA 90740

ANTIONETTE MORELLI
1814 Moreshead Street
San Antonio, TX 78231

MURRY B. MOSKOWITZ
6414 Four Oaks Lane
Burke, VA 22015

JUAN DIEGO HERNANDEZ
18553 Appalossa Drive
Frisco, TX 75035

JAMES F. BIGGERMAN
1233 Stonehenge Way
Shelbyville, IN 46176

ALLIE RICHARDSON
4621 OuterLoop #221

Civil Action No.
1:11-cv-01800-RLW

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Louisville, KY 40219

and

CAROL KELLER
71 N. Marshall Street
Revere, MA 02151

On behalf of themselves and all other similarly situated,

Plaintiffs,

v.

TRICARE MANAGEMENT ACTIVITY
1400 Defense Pentagon
Washington, D.C. 20420

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION
1710 SAIC Drive
McLean, VA 22102

UNITED STATES DEPARTMENT OF DEFENSE
1400 Defense Pentagon
Washington, D.C. 20420

and

LEON E. PANETTA, in his Official Capacity as Secretary of Department of Defense
1400 Defense Pentagon
Washington, D.C. 20420

Defendants.

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Virginia Gaffney, Jessica Palmer, minor H.P., minor C.P., minor C.P. III, Shanna Hartman, Antoinette Morelli, Murry B. Moskowitz, Juan Diego Hernandez, James Biggerman, Allie Richardson, and Carol Keller (collectively "Plaintiffs"), on behalf of themselves and all other persons similarly situated, bring the following action against Defendant TRICARE Management Activity ("TRICARE"), the agency administering the TRICARE health

care program to Uniformed Service members, retirees and their families; Science Applications International Corporation ("SAIC"), the government contractor for TRICARE; the United States Department of Defense ("DOD"), and Leon Panetta, in his Official Capacity as Secretary of the DOD ("Secretary of DOD" or "Secretary") (collectively, "Defendants"), based upon personal knowledge as to their own acts, and, as to all other matters, upon information and belief:

NATURE OF THE ACTION

1. This action seeks to redress Defendants' intentional, willful, and reckless violations of the privacy rights of more than 4.9 million individuals who entrusted their private medical and other personal information to Defendants. Defendants betrayed that trust by failing to properly safeguard this private information and by publicly disclosing it in violation of numerous laws, including, *inter alia*, the federal Administrative Procedures Act ("APA"), the Fair Credit Reporting Act ("FCRA"), the federal Privacy Act of 1974 ("Privacy Act"), various state and District of Columbia laws, and the common law.

2. Defendant TRICARE provides health insurance to millions of military personnel and their families. As a result, TRICARE is entrusted with private medical and personal information for millions of people who are serving or have faithfully served our country. TRICARE is required to safeguard and maintain the privacy of this information pursuant to numerous laws and regulations, including the APA and the Privacy Act.

3. Defendant DOD contracts with Defendant SAIC to provide a variety of services, including data security services for TRICARE beneficiaries' personally identifiable and protected health information. Pursuant to these contracts, DOD pays SAIC tens of millions of dollars per year. In May 2011, DOD contracted with SAIC to provide these services under a

three-year options contract valued at $53 million. On or about February 6, 2012, after the unlawful data disclosure in question, DOD again extended its contract with SAIC.

4. On or about September 29, 2011, TRICARE publicly admitted that on September 12, 2011, data containing the most highly sensitive personal and intimate information pertaining to 4.9 million of its members was unlawfully disclosed ("Security Breach" or "disclosure"). This wrongly disclosed confidential information included Social Security numbers, addresses, dates of birth, phone numbers, and personal health data including private medical records, provider information, laboratory test results, and prescription information ("Confidential Information").

5. Defendants flagrantly disregarded Plaintiffs' privacy rights by intentionally, willfully, and recklessly failing to take the necessary precautions required to safeguard the Confidential Information of 4.9 million people from unauthorized disclosure. In violation of federal law, the information was unprotected, easily copied, and not kept in accordance with basic security protocols. Defendants inexplicably failed to properly encrypt the information, and then intentionally, recklessly, and willfully allowed an untrained or improperly trained individual to access the Confidential Information. Defendants compounded their dereliction of duty by authorizing an untrained or improperly trained individual to remove the improperly encrypted Confidential Information from governmental premises and leave it for almost eight hours in an unguarded car parked in a public location, resulting in its theft by an unknown party or parties.

6. Defendants' intentional, willful, and reckless disregard of Plaintiffs' privacy rights caused one of the largest unauthorized disclosures of Social Security numbers, medical records, and other private information in recent history.

7. On December 2, 2011, five members of Congress wrote a scathing letter to TRICARE regarding the Security Breach that, *inter alia*, criticizes Defendants' conduct in

allowing the wrongful disclosure to occur ("Congressional Letter"). *See* Letter from Congress Members Markey, Barton, Degette, Stearns and Andrews to TRICARE, Dec. 2, 2011, a*vailable at*: http://markey.house.gov/docs/2011_1202_letter_to_director_of_tricare.pdf.

8. The Congressional Letter expresses Congress' "deep concerns about a major breach of personally identifiable and protected health information," and accurately states that "[t]his breach by a firm responsible for handling the military health provider's patient data represents an extremely serious and substantial lapse in security."

9. The Congressional Letter poses numerous questions about the security defects that caused the Security Breach. Although the letter demands a written response by February 2, 2012, TRICARE has failed to comply with the two month deadline and has yet to provide Congress with a written response.

10. As a direct result of the Security Breach, Plaintiffs Ms. Morelli, Mrs. Keller, Mr. Hernandez, and Mr. Biggerman (along with countless other Class members) have been the victims of fraud and identity theft and been harmed thereby.[1] Others, including Mr. Biggerman and Mr. Moskowitz, were subjected to a significant increase in unwanted solicitations from telemarketers who suddenly obtained their confidential personal identification information, including contact information, soon after the disclosure. Still others, including Mrs. Gaffney, have dealt with credit card cancellations. As a result of Defendants' actions, the victims of the Security Breach incurred uncompensated costs and expenses, including the direct costs

[1] The Government Accounting Office stated that "identity theft" is a broad term encompassing various types of criminal activities. Generally, identity theft occurs when a person's identifying information is used to commit fraud or other crimes. These crimes include credit card fraud, phone or utilities fraud, bank fraud, and government fraud.

associated with fraud and identity theft and the cost of purchasing credit reports and/or credit monitoring services.

11. Defendants' actions have also placed Plaintiffs and the proposed Class Members at imminent, immediate and substantial risk of identity theft-related harm. This risk can be quantified. Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, created the 2010 Identity Fraud Survey Report ("the Javelin Report") to quantify the effects of data breaches. The Javelin Report reveals that individuals whose information is subject to a reported data breach, like Plaintiffs, are approximately four times more likely than the general public to be suffer fraud or identity theft. Unfortunately, it appears that victims of the Security Breach have suffered identity theft at a rate that is even higher than that suffered by people who were victimized by other data breaches. The high rate of identity theft among victims of the disclosure is striking, especially given (i) the fact that Defendants possess much of the relevant data, (ii) the likelihood that significant identity theft and fraud has not yet been discovered or reported, and (iii) the possibility that criminals who may have obtained the victims' confidential information have not yet used that information, but will do so at a later date.

PARTIES

12. Plaintiff Virginia E. Gaffney ("Mrs. Gaffney") is the spouse of a decorated war veteran. Mrs. Gaffney has received insurance through TRICARE since prior to 1992. TRICARE possesses Mrs. Gaffney's most sensitive personal and medical information, which, pursuant to federal law, Defendants are required to keep confidential. As a result of Defendants' unlawful conduct, Mrs. Gaffney's medical information and personal information, including her Social Security number, have been exposed, and she has suffered economic loss and other actual

harm. For example, Mrs. Gaffney holds credit cards through USAA bank, which serves millions of military veterans and family members. Shortly after the Security Breach, USAA cancelled one of Mrs. Gaffney's credit cards, based on allegedly "suspicious activity." Based upon the timing of the card cancellation and Mrs. Gaffney's history with her USAA credit card, it is likely that the cancellation was caused by the Security Breach. Mrs. Gaffney suffered embarrassment when she learned of the cancellation when her card was rejected at a restaurant; she was further inconvenienced by the process of getting a new card. Additionally, Mrs. Gaffney purchased a credit and personal identity monitoring service to alert her to potential misappropriation of her identity and to combat risk of further identity theft, and thus has suffered economic loss that is at minimum equal to the cost of the monitoring service. Mrs. Gaffney has also suffered emotional distress as a result of the invasion of her privacy. Finally, as further discussed herein, exposure of Mrs. Gaffney's medical and other personal information has placed her at imminent, immediate, and continuing risk of further identity theft-related harm.

13. Plaintiff Jessica Palmer ("Mrs. Palmer") is the spouse of an Air Force officer. Mrs. Palmer has received insurance through TRICARE since 2005. TRICARE possesses Mrs. Palmer's most sensitive personal and medical information, which, under the law, Defendants are required to keep confidential. As a result of Defendants' unlawful conduct, Mrs. Palmer's medical information and personal information, including her Social Security number, have been exposed, and Mrs. Palmer has suffered economic loss and other actual harm. For example, Mrs. Palmer and her husband purchased a credit and personal identity monitoring service on her own behalf and on behalf of the family to alert her to potential misappropriation of her identity, and thus have suffered economic loss that is at minimum equal to the cost of the monitoring service. Mrs. Palmer has also suffered emotional distress as a result of the invasion of her privacy.

Finally, as further discussed herein, exposure of Mrs. Palmer's medical and other personal information has placed her at imminent, immediate, and continuing risk of further identity theft-related harm.

14. Plaintiff "H.P." is the fourteen-year-old girl daughter of an Air Force officer. Pursuant to Federal Rule of Civil Procedure 17, H.P. is represented by and appears in this action through her stepmother and guardian, Mrs. Palmer. H.P. has received insurance through TRICARE for her entire life. TRICARE possesses H.P.'s most sensitive personal and medical information, which, under the law, Defendants are required to keep confidential. As a result of Defendants' unlawful conduct, H.P.'s medical information and personal information, including her Social Security number, have been exposed, and H.P.'s family has suffered economic loss and other actual harm. For example, H.P.'s family purchased a credit and personal identity monitoring service on her behalf to alert them to potential misappropriation of her identity and thus have suffered economic loss at minimum equal to the cost of the monitoring service. H.P. has also suffered emotional distress as a result of the invasion of her privacy. Finally, as further discussed herein, exposure of H.P's medical and other personal information has placed her at imminent, immediate, and continuing risk of further identity theft-related harm.

15. Plaintiff "C.P." is the five-year-old girl daughter of an Air Force officer. Pursuant to Federal Rule of Civil Procedure 17, C.P. is represented by and appears in this action through her mother and natural guardian, Mrs. Palmer. C.P. has received insurance through TRICARE for her entire life. TRICARE possesses C.P.'s most sensitive personal and medical information, which, under the law, Defendants are required to keep confidential. As a result of Defendants' unlawful conduct, C.P.'s medical information and personal information, including her Social Security number, have been exposed, and C.P.'s family has suffered economic loss and other

actual harm. For example, C.P.'s family purchased a credit and personal identity monitoring service on her behalf to alert them to potential misappropriation of her identity and thus have suffered economic loss at minimum equal to the cost of the monitoring service. C.P. will foreseeably suffer emotional distress as a result of the invasion of her privacy, and her family members have been harmed by their worries about the invasion of her privacy. Finally, as further discussed herein, exposure of C.P.'s medical and other personal information has placed her at imminent, immediate, and continuing risk of further identity theft-related harm.

16. Plaintiff "C.P. III" is the one-year-old boy son of an Air Force officer. Pursuant to Federal Rule of Civil Procedure 17, H.P. is represented by and appears in this action through his mother and natural guardian, Mrs. Palmer. C.P. III has received insurance through TRICARE for his entire life. TRICARE possesses C.P. III's most sensitive personal and medical information, which, under the law, Defendants are required to keep confidential. As a result of Defendants' unlawful conduct, C.P. III's medical information and personal information, including his Social Security number, have been exposed, and C.P.III's family has suffered economic loss and other actual harm. For example, C.P.'s family purchased a credit and personal identity monitoring service on his behalf to alert them to potential misappropriation of his identity and thus have suffered economic loss that is at minimum equal to the cost of the monitoring service. C.P. III will foreseeably suffer emotional distress as a result of the invasion of his privacy, and his family members have been harmed by their worries about the invasion of his privacy. Finally, as further discussed herein, exposure of C.P.'s medical and other personal information has placed him at imminent, immediate, and continuing risk of further identity theft-related harm.

17. Plaintiff Shanna Hartman ("Mrs. Hartman"), a California resident, is the spouse of a highly decorated Senior Chief in the Navy who has served in combat zones. Mrs. Hartman, together with her husband and their six children, has received insurance through TRICARE since 2000. TRICARE possesses Mrs. Hartman's most sensitive personal and medical information, which, under the law, Defendants are required to keep confidential. As a result of Defendants' unlawful conduct, Mrs. Hartman's medical information and personal information, including her Social Security number, have been exposed, and she has suffered economic loss and other actual harm. Mrs. Hartman has suffered emotional distress as a result of the invasion of their privacy. As further discussed herein, exposure of Mrs. Hartman's medical and other personal information has placed her, her husband and her six children at imminent, immediate, and continuing risk of further identity theft-related harm.

18. Plaintiff Antoinette Morelli ("Ms. Morelli") is an Air Force veteran and thespouse of a retired Air Force Colonel. Both Ms. Morelli and her husband served in the first Gulf War. Ms. Morelli was wounded during the Gulf War and is a disabled veteran. As a retired veteran, Ms. Morelli is a TRICARE beneficiary, and TRICARE possesses Ms. Morelli's most sensitive personal information and medical information, which, under the law, Defendants are required to keep confidential. As a result of Defendants' unlawful conduct, Ms. Morelli's medical information and personal information, including her Social Security number, have been exposed, and she has suffered economic loss and other actual harm. For example, in the weeks following the security breach, Ms. Morelli and her spouse experienced unauthorized charges on two credit cards and unauthorized withdrawals from two bank accounts. In response to notifications following the disclosure that certain financial accounts have been compromised, Ms. Morelli and her husband have had to: (a) cancel credit cards and close bank accounts; (b) open new credit

cards and bank accounts; (c) stop direct deposits to those compromised accounts; (d) re-enroll in direct deposits for new accounts; (e) stop recurring electronic payments made from compromised accounts; and (f) re-enroll in electronic payments through new accounts. Additionally, Ms. Morelli purchased a credit and personal identity monitoring service to alert her to potential misappropriation of her identity and to combat risk of further identity theft, and thus has suffered economic loss that is at minimum equal to the cost of the monitoring service. Ms. Morelli has also suffered emotional distress as a result of the invasion of her privacy. Finally, as further discussed herein, exposure of Ms. Morelli's medical and other personal information has placed her at imminent, immediate, and continuing risk of further identity theft-related harm.

19. Plaintiff Murry B. Moskowitz ("Mr. Moskowitz") is a retired Air Force Major. As a TRICARE member, Mr. Moskowitz has used and continues to use TRICARE participating physicians, laboratories, and hospitals in Virginia and elsewhere. TRICARE possesses Mr. Moskowitz's most sensitive personal and medical information, which, under the law, Defendants are required to keep confidential. As a result of Defendants' unlawful conduct, Mr. Moskowitz's medical information and personal information, including his Social Security number, have been exposed and he has suffered economic loss and other actual harm. For example, shortly after the disclosure, Mr. Moskowitz began receiving a number of unsolicited calls from telemarketers and scam artists. Other Class Members also report an increase in unsolicited calls, and it is very possible that the thieves have sold Mr. Moskowitz's personal identification information, possibly through two or three steps, to telemarketers. Mr. Moskowitz has been inconvenienced by these unwanted calls. Mr. Moskowitz has also suffered emotional distress as a result of the invasion of his privacy. Finally, as further discussed herein, exposure of the medical and other personal

information of Mr. Moskowitz and his spouse has placed them at imminent, immediate, and continuing risk of further identity theft-related harm.

20. Plaintiff Juan Diego Hernandez ("Mr. Hernandez") is retired from serving in the Army. As a retired veteran, Mr. Hernandez is a TRICARE beneficiary, and TRICARE possesses Mr. Hernandez's most sensitive personal and medical information, which, under the law, Defendants are required to keep confidential. Mr. Hernandez's spouse is also a TRICARE beneficiary. As a result of Defendants' unlawful conduct, Mr. Hernandez's medical information and personal information, including his Social Security number, have been exposed, and he has suffered economic loss and other actual harm. For example, in October 2011, Mr. Hernandez noticed fraudulent charges on the credit card account he holds with his spouse. Mr. Hernandez spent several hours calling the bank and providing information to remedy these fraudulent charges. In addition to the costs and time spent remedying fraudulent charges, Mr. Hernandez and his spouse have suffered emotional distress as a result of the invasion of their privacy. Finally, as further discussed herein, exposure of the medical and other personal information of Mr. Hernandez and his spouse has placed them at imminent, immediate, and continuing risk of further identity theft-related harm.

21. Plaintiff James Biggerman ("Mr. Biggerman") is a retired Commander Sergeant Major with the Army. As a retired veteran, Mr. Biggerman is a TRICARE beneficiary, and TRICARE possesses Mr. Biggerman's most sensitive personal and medical information, which, under the law, Defendants are required to keep confidential. As a result of Defendants' unlawful conduct, Mr. Biggerman's medical information and personal information, including his Social Security number, have been exposed, and he has suffered economic loss and other actual harm. For example, in January 2012, Mr. Biggerman was notified about fraudulent charges on his

credit card account. Mr. Biggerman spent several hours of his time remedying these fraudulent charges. Additionally, shortly after the disclosure, Mr. Biggerman began receiving a number of unsolicited calls from telemarketers and scam artists. Other Class Members also report an increase in unsolicited calls, and it is very possible that the thieves have sold Mr. Biggerman's personal identification information, possibly through two or three steps, to telemarketers. Mr. Biggerman has been inconvenienced by these unwanted calls. Mr. Biggerman has purchased a credit and personal identity monitoring service to alert him to potential misappropriation of his identity and to combat risk of further identity theft, and thus has suffered economic loss that is at minimum equal to the cost of the monitoring service. Mr. Biggerman has also suffered additional emotional distress as a result of the invasion of his privacy. Finally, as further discussed herein, exposure of Mr. Biggerman's medical and other personal information has placed him at imminent, immediate, and continuing risk of further identity theft-related harm.

22. Plaintiff Allie Richardson ("Mr. Richardson") is a retired member of the armed forces. As a retired veteran, Mr. Richardson and his wife are TRICARE beneficiaries, and TRICARE possesses Mr. Richardson's most sensitive personal and medical information, which, under the law, Defendants are required to keep confidential. As a result of Defendants' unlawful conduct, Mr. Richardson's medical information and personal information, including his Social Security number, have been exposed, and he has suffered economic loss and other actual harm. For example, Mr. Richardson purchased a credit and personal identity monitoring service on his own behalf and on behalf of his family to alert him to potential misappropriation of his identity and to combat risk of further identity theft, and thus he and his wife have suffered economic loss that is at minimum equal to the cost of the monitoring service. Mr. Richardson has also suffered emotional distress as a result of the invasion of his privacy. Finally, as further discussed herein,

exposure of Mr. Richardson's medical and other personal information has placed him at imminent, immediate, and continuing risk of future identity theft-related harm.

23. Plaintiff Carol Keller ("Mrs. Keller") is married to a retired disabled veteran of the Air Force. As the spouse of a retired veteran, Mrs. Keller is a TRICARE beneficiary, and TRICARE possesses Mrs. Keller's most sensitive personal and medical information, which, under the law, Defendants are required to keep confidential. As a result of Defendants' unlawful conduct, Mrs. Keller's medical information and personal information, including her Social Security number, have been exposed, and she has suffered economic loss and other actual harm. For example, since the time of the disclosure, Mrs. Keller has discovered three separate instances of fraudulent charges on her debit card and bank accounts – one in October 2011, one in December 2011, and one in January 2012. Mrs. Keller and her husband have spent many hours remedying these fraudulent charges and communicating with her debit card banks. Additionally, Mrs. Keller has a sensitive medical condition which has been disclosed as a result of the Security Breach, and the revelation of her condition has caused her and her spouse to suffer an inordinate amount of emotional distress. Finally, as further discussed herein, the exposure of the medical and other personal information of Mrs. Keller and her spouse has placed them at imminent, immediate and continuing risk of further identity theft-related harm.

24. Defendant TRICARE is an agency within the Military Health System, the fully integrated healthcare system of the DOD, and is therefore an "agency" for purposes of the Privacy Act. TRICARE provides health-care coverage for medical services, medication, and dental care for military personnel, families, retirees, and their survivors. TRICARE is entrusted with highly confidential medical and personal records for millions of members of the armed services and their families.

25. Defendant DOD is an executive department of the federal government and is, therefore, an "agency" for purposes of the Privacy Act. Defendant DOD is entrusted with highly confidential and personal records of millions of citizens who bravely serve or have served our country, as well as their families' records.

26. Defendant Leon E. Panetta , in his Official Capacity as Secretary of the DOD ("Secretary" or "Secretary of the DOD"), is the official responsible for the proper execution and administration of all laws administered by the DOD and for the control, direction, and management of the DOD.

27. Defendant SAIC is a Delaware corporation and maintains primary offices in McLean, Virginia, and additional offices throughout the United States. SAIC derives a substantial amount of its revenue from DOD contracts – in the last three fiscal years SAIC has been given over $20 billion from DOD pursuant to contracts. DOD contracts with and pays SAIC tens of millions of dollars per year to provide data security services for TRICARE beneficiaries' Confidential Information. Recently, DOD contracted with SAIC to provide data security services under an options contract for three years valued at $53 million.

28. Defendant SAIC is a Consumer Reporting Agency as defined under the FCRA because Defendant regularly engages, in whole or in part, in the practice of assembling information on consumers for the purpose of furnishing consumer reports to third parties and/or uses interstate commerce for the purpose of preparing and/or furnishing consumer reports.

JURISDICTION AND VENUE

29. The jurisdiction of this Court arises pursuant to 28 U.S.C. § 1331 because this is a civil action arising under the laws of the United States. This court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d). Jurisdiction is also proper pursuant to 5 U.S.C. §§

552a(g)(1), (5) because this is a civil action to enforce a liability created under 5 U.S.C. § 552a after September 27, 1975.

30. Venue is appropriate in this Court pursuant to 28 U.S.C. § 1391 because all Defendants are subject to the personal jurisdiction of this District and a substantial part of the events or omissions giving rise to the claims occurred in this district.

SUBSTANTIVE ALLEGATIONS

A. Factual Background

31. As an agency within the Military Health System of the DOD, TRICARE manages a fully integrated health care system that provides health care coverage, prescription services, and dental care for military personnel, retirees, their families, and anyone else entitled to health benefits from the DOD. TRICARE has performed these duties since February 1998, and, in doing so, TRICARE and DOD are obligated to protect the private and sensitive personally identifiable and protected health information of TRICARE beneficiaries.

32. TRICARE manages health coverage for approximately 9 million individuals. These individuals are organized into three regions: North, South, and West, with each region containing approximately 3 million beneficiaries.

33. TRICARE and DOD are legally obligated to maintain the secrecy of Confidential Information in accordance with all applicable laws and are responsible for hiring and contracting any third party entrusted by TRICARE and DOD to perform these same duties on their behalf.

34. Indeed, in marketing to Plaintiffs, TRICARE pledges to maintain the privacy of members' Confidential Information pursuant to its obligations under federal law, including the Health Information Portability and Accountability Act ("HIPAA"). *See* TRICARE's Privacy and Civil Liberties Office notice, *available at:* http://www.tricare.mil/tma/privacy (promising

"compliance with federal privacy and security laws, and Department of Defense (DOD) regulations and guidelines . . .").

35. In 1992, TRICARE and DOD contracted with SAIC as a government contractor entrusted with protecting and safeguarding Confidential Information received by TRICARE and DOD. As a government contractor, SAIC has a duty to ensure the secrecy of Confidential Information and to carry out its duties in accordance with the Privacy Act and APA.

36. SAIC's website boasts that SAIC "preserv[es] confidentiality, data integrity, and service availability." SAIC Security and Privacy, *available at*: http://www.saic.com/health/healthit/security-privacy.html.

37. Over the three previous fiscal years, SAIC has received more than $20 billion in federal contracts, including those paid by TRICARE and DOD.

38. On May 19, 2011, SAIC announced that it was awarded a prime contract by DOD to provide information technology services and electronic health records system support to TRICARE. The contract provides for three one-year options under which DOD will pay SAIC a total of $53 million if all options are exercised.

39. Indeed, on or about February 6, 2012, the DOD extended the sole-source contract with SAIC to continue with the very same duties which, as evidenced by the Security Breach and other breaches discussed more fully herein, SAIC has repeatedly failed to adequately perform. NextGov, a website that monitors technology and government, described the absurdity of this extension:

> File this one under irony. Science Applications International Corp., the outfit that jeopardized the health care records of 4.9 million TRICARE beneficiaries when computer tapes containing the data were stolen from an employee's car, just received a sole-source contract to continue supporting the Defense Department core electronic health record system. . . . What is unusual is there

> is no time line and no value given for this extension, a rather glaring omission considering SAIC's poor stewardship of records.

SAIC Wins More TRICARE Business, *available at*:

http://whatsbrewin.nextgov.com/2012/02/saic_wins_more_tricare_business.php. Absent litigation, it is clear that the DOD and SAIC would continue to fail to safeguard the Confidential Information of military members and their families in perpetuity.

B. DOD and SAIC Knew the DOD's Information Security Systems Were Not Secure

40. In order to secure and safeguard confidential information maintained by the federal government, the Federal Information Security Management Act ("FISMA"), along with the General Accounting Office, requires that each federal agency, including the DOD, create a report addressing the agency's risk-based approach to agency-wide information security management. FISMA and the GAO then release annual scorecards based on the FISMA reports submitted by the agencies.

41. In March of 2006, the 2005 FISMA grades were released. The DOD received a grade of "F," the same grade received by the DOD in 2001 and 2002 and down from the FISMA grade of "D" that the DOD received in 2004. *See* FISMA Computer Security Report Card, March 16, 2006, attached as Exhibit A ("2006 FISMA Report"). The 2006 FISMA Report noted that "[o]ur analysis reveals that the scores for the Departments of Defense . . . remained unacceptably low or dropped precipitously. . . . If FISMA was the No Child Left Behind Act, a lot of the critical agencies [including the DOD] would be on the list of 'low performers.' None of us would accept D+ grades on our children's report cards. We can't accept these either." Several "areas of concern" for FISMA included "specialized security training for employees with significant security responsibilities" and "agency responsibility for contractors systems." *Id.*

C. SAIC's Prior Security Failures

42. Since 2005, SAIC has experienced no fewer than six security failures due to malware infections, stolen computers, and, last year, another instance of stolen backup tapes.

43. On June 30, 2010, SAIC notified the Maryland Office of the Attorney General that it discovered a theft of backup tapes exposing sensitive private information, including Social Security numbers.

44. On January 1, 2008, SAIC notified the Massachusetts Office of the Attorney General that malware infected a company computer, and, as a result, the credit card information of certain customers was compromised.

45. On July 20, 2007, SAIC announced that the Social Security numbers and personal health records of nearly 900,000 soldiers, their family members, and other government employees – stored on a non-secure computer server – were compromised because SAIC did not encrypt the data that it transmitted online. Then CEO and current Chairman of SAIC, Ken C. Dahlberg, described the 2007 security breach as "completely unacceptable."

46. On February 12, 2005, SAIC notified 45,000 past and present employees – including top military and intelligence officials – that they were at risk of identity theft after computers containing Social Security numbers, financial transaction records, and other sensitive personal information were stolen during a break-in at SAIC's administration building in San Diego, California.

47. This pattern of systemic security failures, along with the consistently failing FISMA grades, demonstrates that SAIC has been unable or unwilling to correct its faulty data protection policies. This pattern of willful and intentional disregard for the security of the data under its control continues although SAIC has experienced repeated warnings and

embarrassments. This is especially troubling considering that SAIC is a corporation that is specifically entrusted to protect the private information of soldiers, retirees, and their families.

48. Although SAIC continually fails to properly perform its statutory and contractual duties to provide adequate protection of sensitive personally identifiable and protected health information, DOD repeatedly rewards SAIC with multi-million-dollar contracts to perform information technology services and electronic health record system support services.

D. Defendants' Latest Security Breach & Wrongful Disclosure

49. On September 29, 2011, TRICARE released a statement on its website concerning a security breach ("September 29 Notification"). According to the statement, more than two weeks prior, on September 14, 2011, TRICARE learned that on September 12, 2011 SAIC had experienced a security breach affecting approximately 4.9 million TRICARE beneficiaries, many of whom received care or had laboratory work processed through military facilities in San Antonio, Texas since 1992 ("Security Breach" or "disclosure").

50. TRICARE stated that the Security Breach resulted in the wrongful disclosure of backup computer tapes from an electronic healthcare record. The personal information on the compromised tapes included Social Security numbers, addresses, phone numbers, dates of birth, and private medical information such as clinical notes, lab tests, prescription information, and private health information for patients located nationwide.

51. The September 29 Notification provided scant details of the types of data stolen and vague descriptions of the persons affected. In refusing to elaborate further, TRICARE explained that "this data loss remains the subject of an ongoing investigation" and that they "did not want to raise undue alarm in [their] beneficiaries and so wanted to determine the degree of risk this data loss represented before making notifications."

52. On or about September 29, 2011, Vernon Guidry ("Guidry"), spokesman for SAIC, confirmed that SAIC was the custodian of the Confidential Information when the disclosure occurred.

53. SAIC has contracted with TRICARE and DOD to provide a variety of services, including data security services, since at least 1992.

54. TRICARE and Guidry confirmed that the wrongfully disclosed backup tapes were being transported "pursuant to contract requirements" with SAIC.

55. On or about September 12, 2011, the backup tapes and records, which were being transported by an SAIC employee, were left in an unattended 2003 Honda Civic for most of the day, from approximately 7:53 a.m. to 4:30 p.m., in a parking garage of an upscale office building with 24-hour security in downtown San Antonio.

56. The parking garage where the Security Breach took place contained many cars that were far more valuable than the 2003 Honda Civic. Yet the thief or thieves, who went to great effort to avoid security, did not break into any of the luxury cars in the garage, targeting instead the relatively inexpensive car containing the confidential data. The thief or thieves stealthily broke into the employee's Honda Civic and took the unencrypted backup tapes and records, thereby gaining information worth billions of dollars.

57. The nature of this theft supports the logical inference that the thief or thieves were specifically targeting the Confidential Information contained on the backup tapes and records.

58. The SAIC employee who failed to properly transport the records did not receive a security background check nor did that employee receive the requisite training mandated by federal law.

59. SAIC placed the employee entrusted to transport the backup tapes on administrative leave, and, according to Guidry, "it was his job to transfer tapes in an expeditious manner between facilities, that's all we're going to say at this point." Guidry would not state whether the employee violated an internal policy by leaving the tapes in his car, but acknowledged, "if they weren't in his car, they wouldn't be stolen."

60. The industry practice in the data security field is to use an armored car to transport such a large amount of sensitive data.

61. Additionally, the backup tapes were not encrypted pursuant to federal standards. SAIC stated that the system that generated the backup tapes was incapable of encrypting the backup tapes pursuant to federal standards.

62. TRICARE's Operations Manual sets forth numerous regulations, with which TRICARE does not comply, including, *inter alia,* that TRICARE will "adopt industry best practices of [electronic personal health information] technologies and management."

63. Upon information and belief, Defendants' policy failures include: (1) failing to properly encrypt computer tapes and other data; (2) providing untrained and/or improperly trained individuals with access to highly sensitive data and allowing those individuals to transport computer tapes and other data; and (3) routinely allowing individuals to transport highly confidential data without taking all precautions mandated by law, including some of the most basic and rudimentary precautions.

64. Defendants knew about these policy failures as early as 2006 when FISMA gave the DOD a grade of "F" and noted several "areas of concern" for the DOD, including "specialized security training for employees with significant security responsibilities" and

"agency responsibility for contractors systems." Yet SAIC's contract has been repeatedly renewed and DOD and SAIC have failed to remedy their inability to properly safeguard records.

65. To date, none of the stolen backup data has been recovered, let alone accounted for.

E. Defendants' Inadequate Post-Disclosure Response

66. According to TRICARE's Operations Manual dated February 1, 2008, TRICARE and its contractors "shall inform affected individuals whenever they become aware that protected personal information pertaining to a Service member, civilian employee, military retiree, family member, or another individual affiliated with [DOD] has been lost, stolen or compromised. Notification will take place as soon as possible, **but not later than ten days after the loss or compromise of protected personal information is discovered**." (Emphasis added.) Despite this policy requirement, Defendants did not provide any information whatsoever to TRICARE members until the September 29 Notification, fifteen days after discovery of the Security Breach. Moreover, the September 29 Notification was not even specifically targeted to TRICARE members but was only directed to the public at large.

67. The September 29 Notification was not only untimely, but the substance was also woefully inadequate. The information provided was obscurely displayed on the TRICARE website and was vague in explaining the details about the Security Breach or those persons affected. As such, the September 29 Notification did not provide adequate notice to impacted persons.

68. There is no proper explanation for the 15-day delay or the inconspicuous, vague September 29 Notification given by Defendants. Approximately a week after the first press release and three weeks after the Security Breach occurred, Defendants announced that specific

notification would be sent by mail, and that such notification would take approximately 6 *additional* weeks to complete. Based upon this publicly disclosed timetable, it would appear Defendants did not specifically notify the majority of affected persons until at least 9 weeks after the breach had occurred.

69. Individual notice was not mailed to TRICARE members until more than two months after the initial disclosure. Unfortunately, this notice was also inadequate, as a large number of Class Members did not receive the mailed notice ("SAIC Letter") and could only confirm that they had been victims of the Security Breach by contacting SAIC directly.

70. Moreover, the SAIC Letter is materially misleading. The letter advises recipients that "[t]he chance that your information could be obtained from these tapes is low . . ." Defendants have admitted, however, that the data on the tapes was improperly encrypted. Accordingly, the Confidential Information is easily available to motivated criminals, and categorizing the risk of access as "low" is misleading as to the imminence of identity theft risk faced by victims of the Security Breach.

71. The SAIC Letter advised its recipients that they may take several steps in response to the disclosure. Unfortunately, many of these steps would force victims of the disclosure to incur additional economic costs. For example, a victim of the disclosure who placed a "security freeze" on her credit report, an option described in the SAIC letter, would likely incur out-of-pocket economic costs of at least $5.00. Similarly, monitoring credit reports, another option described in the SAIC letter, would entail a cost, because victims of the disclosure would have to pay to see credit reports beyond the one free report to which they are entitled annually.

72. Defendants' actions and inactions in failing to timely report the unauthorized disclosure of Confidential Information and personal information were arbitrary, capricious, and without observance of procedures required by law. These actions and inactions took place in numerous locations, including, specifically, the District of Columbia, where Defendants conduct much of their business.

73. Defendants have been repeatedly informed of recurring, systemic, and fundamental deficiencies in information security, but have failed to effectively respond. Despite the repeated identification of problems, Defendants have been unable or unwilling to properly secure the personal information under their control. These repeated failures to correct known vulnerabilities of Defendants' safeguards for Plaintiffs' private information demonstrate a reckless disregard for TRICARE members' privacy rights and intentional or willful violations of applicable laws.

74. In the first month following the breach, Defendants did not offer any assistance to impacted persons. However, in the September 29 Notification, Defendants encourage persons who may have been impacted to "take steps to protect their personal information" and to follow the guidance on the Federal Trade Commission ("FTC") website, which describes the actions that should be taken by consumers in response to identify theft. Essentially, Defendants left the responsibility for remedying the breach to the victims themselves.

75. According to the FTC website, there are four main steps that every person should take when he or she thinks that he or she may have been the victim of identity theft:

(i) Place a fraud alert on the person's credit reports and review credit reports for suspicious activity;

(ii) Close accounts that the person knows or thinks may have been compromised. According to the FTC, these actions may include sending letters and affidavits to financial institutions to have fraudulent charges credited to accounts;

(iii) File a complaint with the FTC, to help law enforcement agencies and provide information to the FTC to help it combat identity theft; and

(iv) File a police report with the person's local or community police department.

Defend: Recover from Identity Theft, *available at*: http://www.ftc.gov/bcp/edu/microsites/idtheft//consumers/defend.html

76. However, Defendants initially offered no direct assistance to those impacted, nor did they explain any steps that were being taken to protect against future wrongful disclosures. In fact, referring Security Breach victims to the FTC website is inconsistent with the impressions created by the substantive content (or lack thereof) contained in the September 29 Notification and subsequent SAIC Letter.

77. After the Defendants were served with class action lawsuits, the first two of which were filed on October 7, 2011 and October 11, 2011 by two of the Plaintiffs' counsel in this case, Defendants completely reversed their position. On or about November 7, 2011, Defendants issued a press release stating that TRICARE and DOD directed SAIC to provide one year of free identity theft monitoring to affected persons.

78. Unfortunately, the protection now offered by the Defendants is woefully inadequate. For the following reasons, among others, the Defendants' offering is insufficient:

(i) Defendants offered a single bureau credit monitoring program that provides no protection to minors. Each minor child victim continues to be fully exposed to damages and Defendants have provided no remedy for such children;

(ii) Defendants do not provide any protection against medical identity theft, the victims of which are often left with huge medical bills, damaged credit, and erroneous medical records. According to a September 2011 report by PwC's Health Resource Institute "Old Data Learns New Tricks," the problem of medical identity theft is worsening and is the fastest growing form of identity theft. Old Data Learns New Tricks, *available at*: http://www.pwc.com/us/en/health-industries/publications/old-data-learns-new-tricks.jhtml The "protection" offered by Defendants does nothing to protect against medical identity theft and fraudulent health insurance claims; and

(iii) The "protection" offered by Defendants lasts only a single year. As reported by the FTC, a person impacted by identity theft should take proactive steps well after a year has passed to protect against identity theft and identity theft related risks.

F. The Harm Defendants Perpetrated on Plaintiffs and the Class

79. Defendants flagrantly disregarded Plaintiffs' privacy rights and harmed Plaintiffs by not obtaining prior written consent of Plaintiffs, or any individual, before disclosing the Confidential Information to any other individual or government agency, as is required by the Privacy Act, the APA, the FCRA, HIPAA, the Health Information Technology for Economic and

Clinical Health Act ("HITECH"), the California Confidentiality of Medical Information Act, and other pertinent laws and regulations.

80. Defendants flagrantly disregarded Plaintiffs' privacy rights and harmed Plaintiffs by failing to observe the procedures required by law for disclosure of private information, including the Confidential Information, without the prior written consent of the affected individuals.

81. Defendants flagrantly disregarded Plaintiffs' privacy rights and harmed Plaintiffs by failing to safeguard the Confidential Information and disclosing, or allowing disclosure of, the Confidential Information to individuals who did not require access to or possession of the Confidential Information in order to carry out their duties and responsibilities.

82. Defendants flagrantly disregarded Plaintiffs' privacy rights and harmed Plaintiffs by failing to keep or maintain an accurate accounting of the disclosures of the Confidential Information.

83. Defendants flagrantly disregarded Plaintiffs' privacy rights and harmed Plaintiffs by failing to make reasonable efforts to assure that the records containing the Confidential Information were accurate, complete, timely, and relevant for Defendants' purposes prior to disseminating a record about an individual to any person other than an agency.

84. Defendants flagrantly disregarded Plaintiffs' privacy rights and harmed Plaintiffs by failing to establish or implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against anticipated threats to the records' security or integrity, which could harm any individual about whom information was maintained. Defendants' security deficiencies allowed, and continue to allow, a single individual to disclose and/or compromise the personal information of millions of citizens.

Defendants' unwillingness or inability to establish and maintain requisite information security is an abuse of discretion and an intentional and willful failure to observe procedures required by law.

85. Defendants flagrantly disregarded Plaintiffs' privacy rights and harmed Plaintiffs by failing to inform Plaintiffs of the loss of their Confidential Information within the ten-day period mandated by Defendants' own regulations. This lack of timely disclosure increased the risk of identity and credit theft, and forced Plaintiffs and other Class Members to take actions to protect themselves, including by purchasing credit reports and credit monitoring services.

86. Defendant Secretary was ultimately responsible for control, direction, and management of the DOD's processes, policies, and procedures for compliance with the Privacy Act and other applicable laws, but failed to ensure that those processes, policies, and procedures were adequately followed by his subordinates. Defendant Secretary knew, or should have known, that DOD had long-standing information security deficiencies that threatened Plaintiffs' privacy rights, but failed to ensure correction or mitigation of those deficiencies.

87. Defendant Secretary flagrantly disregarded Plaintiffs' privacy rights and harmed Plaintiffs by failing to establish and ensure that his subordinates lawfully complied with appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against anticipated threats to the records' security or integrity, which could result in substantial harm to any individual whose information was maintained.

88. Each of Defendants' failures complained of herein has caused Plaintiffs actual harm and adverse effects including, but not limited to, pecuniary damages, economic loss,

mental distress, emotional trauma, inconvenience, loss of peace of mind, embarrassment, and the threat of current and future harm from identify theft, as described in more fully herein.

89. The actual harm and adverse effects, including the imminent and immediate threat of identity theft and similar adverse effects caused by Defendants' unlawful actions and inactions, requires affirmative acts by Plaintiffs to recover peace of mind, emotional stability, and personal security, including, but not limited to: purchasing credit reporting services; frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, and, closing or modifying financial accounts. Plaintiffs have suffered, and will continue to suffer, damages for the foreseeable future.

90. As a direct result of the Defendants' failures, Plaintiffs have purchased credit monitoring services to safeguard the financial identity of themselves and their families.

91. As a direct result of Defendants' failures, Plaintiffs have had to cancel credit cards and close bank accounts; open new credit cards and bank accounts; stop direct deposits to those compromised accounts and re-enroll in direct deposits for new accounts; stop recurring electronic payments from compromised accounts and re-enroll in electronic payments through new accounts; and otherwise spend time and money in mitigation responding to notifications following the wrongful disclosure that certain financial accounts have been compromised.

92. In addition to the pecuniary loss caused by purchasing a credit monitoring service, all of the Plaintiffs suffered emotional harm from the disclosure of their private medical histories, as well as their Social Security numbers and other information that Defendants were legally obligated to keep private.

93. Indeed, victims and potential victims of identity theft spend hundreds of hours in personal time and hundreds of dollars in personal funds to resolve their credit issues. *See*

Defend: Recover from Identity Theft, *available at*: http://www.ftc.gov/bcp/edu/microsites/idtheft//consumers/defend.html; Fight Identity Theft, *available at*: www.fightidentitytheft.com. According to Javelin, not only is the drastically increased incidence of imminent identity theft a virtual statistical certitude, data breach victims who suffer from identity theft or fraud experience an average fraud-related economic loss of $1,915. Moreover, after spending many hours attempting to rectify the fraud, a typical victims still spends $541 out-of-pocket.

94. Other statistical analyses are in accord. The Government Accounting Office ("GAO") has stated that identity thieves can use identifying data such as Social Security numbers to open financial accounts and incur charges and credit in a person's name. As the GAO has stated, this type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim's credit rating. Moreover, unlike other of the Confidential Information, Social Security Numbers are even more difficult to change and their misuse can continue for years into the future.

95. Identity thieves also use Social Security numbers to commit other sorts of fraud, such as obtaining false identification cards, obtaining government benefits in the victim's name, committing crimes, or filing fraudulent tax returns on the victim's behalf. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

96. The release of Social Security numbers are particularly damaging because identity thieves are able to not only fraudulently open credit card accounts and to obtain loans, but to fraudulently access consumers' existing accounts. Social Security numbers, however, cannot be easily changed like a credit card account number. If an individual's Social Security number has

been compromised, it is much more difficult to protect against identity theft than it would be if credit card information were stolen. Even if an individual overcomes the barriers to changing the social security number, the defensive measure is still not a guarantee of protection against identity theft. The monitoring and preventative efforts that go into protecting oneself against identity theft once confidential information is stolen are costly and raise yet another measure of damages for individuals.

97. Identity theft crimes often encompass more than just immediate financial loss. Identity thieves often hold onto stolen personal and financial information for several years before using and/or selling the information to other identity thieves.

G. Defendants Did Not Comply With Basic Security Protocols For Protecting Confidential Information

98. Federal and state legislatures have passed laws to ensure companies protect the security of sensitive personally identifying confidential information, such as that wrongfully disclosed by Defendants.

99. The FTC has issued a publication entitled "Protecting Personal Information: A Guide for Business" ("FTC Report"). The FTC Report provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes of identity theft. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow the following guidelines:

a. Keep inventory of all computers and laptops where the company stores sensitive data;

b. Do not collect confidential personal identifying information if there is no legitimate business need. If there is a legitimate business need, only keep the information as long as necessary;

c. Use social security numbers only for required and lawful purposes and do not store these numbers unnecessarily, such as for an employee or customer identification number;

d. Encrypt the confidential personal identifying information particularly if the sensitive information is shipped to outside carriers or contractors. In addition, the business should keep an inventory of all the information it ships;

e. Do not store sensitive computer data on any computer with an Internet connection unless it is essential for conducting the business;

f. Control access to sensitive information by requiring that employees use "strong" passwords; tech security experts believe the longer the password, the better; and

g. Implement information disposal practices reasonable and appropriate to prevent an unauthorized access to personally identifying information.

100. The FTC Report also instructs companies that outsource any business functions to proactively investigate the data security practices of the outsourced company and examine their standards.

101. In September 2008, The President's Identity Theft Task Force Report was issued. Therein, it was noted that "[p]ublic concerns about the security of personal information and identity theft remain at high levels, with potentially serious consequences for the functioning of our economy." The President's Identity Theft Task Force Report, *available at*: http://www.ftc.gov/os/2008/10/081021taskforcereport.pdf, at viii.

PROCEDURAL HISTORY

102. Defendants' negligence injured over 4.9 million people. As a result, Plaintiffs filed suit. The first lawsuit against SAIC, *Adcock v. SAIC*, No. 3-11-cv-49, was filed in the

Northern District of Florida on October 7, 2011. The first lawsuit against TRICARE, *Gaffney et al, v. TRICARE et al*., No. 1-11-cv-01800-RLW, was filed in this Court on October 11, 2011. Numerous lawsuits have been filed subsequently, all but two of which are consolidated in the instant complaint.

103. At the time when *Adcock* and *Gaffney* were filed, Defendants refused to provide any services to mitigate the harm caused by the disclosure.

104. However, on November 4, 2011, Defendants suddenly reversed course and offered one year of free credit monitoring to victims of the disclosure. As set forth above, the credit monitoring offered by Defendants is woefully insufficient in that, *inter alia*, (i) it provides no protection for minors; (ii) it provides no protection against medical identity theft; and (iii) it lasts for only one year. Nonetheless, it is significant that Defendants made this offer only after the onset of litigation, when they realized they could not avoid responsibility for their transgressions.

CLASS ACTION ALLEGATIONS

105. Plaintiffs bring this action under Rule 23 of the Federal Rules of Civil Procedure on their own behalf and as representatives of a Class of similarly situated consumers who were all impacted by the Defendants' actions and inactions.

106. Plaintiffs seek to represent a Class defined as follows:

> All natural persons within the United States whose personal information was contained on the tapes that were stolen from an SAIC's employee's car on or about September 12, 2011, in San Antonio, Texas. Excluded from the Class are Defendants, any entity in which any Defendant has a controlling interest, Defendants' legal representatives, heirs, successors, and assigns.
>
> ("Class" or, taken together, "Class Members")

107. Plaintiffs seek to represent a subclass of the Class defined as follows:

> All natural persons within California whose personal information was contained on the tapes that were stolen from an SAIC's employee's car on or about September 12, 2011, in San Antonio, Texas. Excluded from the Class are Defendants, any entity in which any Defendant has a controlling interest, Defendants' legal representatives, heirs, successors, and assigns."
>
> ("California subclass")

108. Plaintiffs seek to represent an additional subclass of the Class defined as follows:

> All natural persons within the District of Columbia whose personal information was contained on the tapes that were stolen from an SAIC's employee's car on or about September 12, 2011, in San Antonio, Texas. Excluded from the Class are Defendants, any entity in which any Defendant has a controlling interest, Defendants' legal representatives, heirs, successors, and assigns."
>
> ("D.C. subclass")

109. Plaintiffs seek to represent an additional subclass of the Class defined as follows:

> All natural persons within any state containing a privately enforceable data breach notification statute that SAIC violated after the disclosure (including Alaska, Connecticut, Hawaii, Illinois, Iowa, Louisiana, Maryland, New Hampshire, North Carolina, Rhode Island, South Carolina and Washington) whose personal information was contained on the tapes that were stolen from an SAIC's employee's car on or about September 12, 2011, in San Antonio, Texas. Excluded from the Class are Defendants, any entity in which any Defendant has a controlling interest, Defendants' legal representatives, heirs, successors, and assigns."
>
> ("Multistate subclass")

110. The members of the Class and subclasses are so numerous that their joinder herein is impracticable. On information and belief, Plaintiffs believe that the total number of members of the Class numbers approximately 4.9 million.

111. The precise number of proposed Class Members and their addresses are currently unknown to Plaintiffs, but can be ascertained from Defendants' records. Class Members can be

notified, if so Ordered by the Court, by mail, supplemented by published notice, if deemed necessary.

112. There are questions of law and fact common to the Class as a whole. These common questions of law and fact predominate over any questions affecting only individual members of the Class. The common questions of law and fact include, but are not limited to:

(a.) Whether Defendants had inadequate security that failed to secure the confidential information and/or permitted the disclosure of the Class's Confidential Information;

(b.) Whether Defendants TRICARE, DOD and Secretary's actions and failures to properly safeguard Plaintiffs' and the Class' sensitive private information were willful, reckless, arbitrary, capricious, and otherwise not in accordance with the law;

(c.) Whether Defendants failed to inform Plaintiffs and Class Members of the wrongful disclosure in a reasonable time and manner;

(d.) Whether SAIC breached its contracts to protect and maintain the safety and security of patients' private information;

(e.) Whether Plaintiff and Class Members are third party beneficiaries of SAIC's contract with TRICARE; and

(f.) Whether Defendants' conduct violated applicable laws.

113. Plaintiffs' claims are typical of the claims of the Class they represent because Plaintiffs, like all Class Members, have been the victims of Defendants' inadequate security and have suffered damages thereby.

114. Plaintiffs will adequately represent the Class because Plaintiffs' interests are common with the other Class Members. Plaintiffs and the other Class Members were commonly harmed by the same practices and policies of Defendants. Plaintiffs' interests do not conflict with the interests of the Class they seek to represent.

115. Plaintiffs have retained counsel who are competent and experienced in the prosecution of both complex civil litigation and class actions.

116. Class certification, therefore, is appropriate pursuant to Fed. R. Civ. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

117. Class certification to obtain injunctive and equitable relief pursuant to Fed. R. Civ. P. 23(b)(2) is also appropriate because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive and equitable relief with respect to the Class as a whole.

118. The prosecution of separate actions by members of the Class would create a risk of establishing incompatible standards of conduct for Defendants. For example, one court might decide that the challenged actions are illegal and enjoin Defendants, while another court might decide that those same actions are not illegal. Individual actions may, as a practical matter, be dispositive of the interest of the Class, whose members would not be parties to those actions.

119. Defendants' actions are generally applicable to the Class as a whole, and Plaintiffs seek, *inter alia*, equitable remedies with respect to the Class as a whole.

120. Defendants' systemic policies and practices make declaratory relief with respect to the Class as a whole appropriate.

121. A class action is superior to other available means for the fair and efficient adjudication of this controversy. The damages suffered by individual members of the Class are small compared to the burden and expense of individual prosecution of the complex and

extensive litigation required to address Defendants' conduct. Absent the class action, the members of the Class will continue to suffer harm.

122. Class action treatment of this litigation is superior to individual litigation because it would be virtually impossible for the members of the Class individually to effectively seek redress for the wrongs done to them by Defendants. Even if the members of the Class could individually bear the financial burden of this litigation, which many cannot, the court system would be excessively burdened given the size of the Class. Individual lawsuits would increase the delay and expense of all the parties and the courts. Individual lawsuits present the potential for inconsistent or contradictory judgments. By contrast, class action treatment presents far fewer management difficulties, allows the hearing of claims, which might otherwise go unaddressed, and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

Count 1: Violation of the Administrative Procedures Act, 5 U.S.C. § 706, *et seq.* Against Defendants TRICARE, DOD, and Secretary

123. Plaintiffs incorporate by reference those paragraphs set forth above as if fully set forth herein.

124. Defendants TRICARE, DOD, and Secretary possess and are charged with maintaining the privacy of personal information of Plaintiffs and the Class. TRICARE, DOD, and Secretary have repeatedly demonstrated an inability or unwillingness to implement, or callous disregard for, fundamental procedures to provide minimally acceptable safeguards to prevent against the disclosure of the sensitive personal information entrusted to their possession.

125. Defendant Secretary is ultimately responsible in his official capacity for safeguarding citizens' private information under DOD control pursuant to the applicable laws,

including the Privacy Act and APA, but has been unable or unwilling to ensure compliance with those laws.

126. Defendants TRICARE, DOD, and Secretary's actions and failures to act in a manner to safeguard Plaintiffs' and the Class' sensitive private information were willful, reckless, arbitrary, capricious, and otherwise not in accordance with the law.

127. Plaintiffs and the Class have suffered, and continue to suffer harm as a proximate result of Defendant TRICARE, DOD, and Secretary's actions, inactions, and delays.

128. Plaintiffs and the Class are entitled to equitable relief, and any other relief to which they are entitled, for Defendant TRICARE, DOD, and Secretary's violation of Plaintiffs' and the Class' rights under the APA.

Count 2: Violation of the Privacy Act of 1974, 5 U.S.C. § 552a *et seq.*
Against Defendants TRICARE, DOD, and Secretary

129. Plaintiffs incorporate by reference those paragraphs set forth above as if fully set forth herein.

130. Defendants TRICARE, DOD, and Secretary violated the Privacy Act.

131. Pursuant to the Privacy Act, an intentional and/or willful violation occurs when a party exhibits patently egregious and unlawful behavior.

132. Each of Defendants TRICARE, DOD, and Secretary's Privacy Act violations, which resulted from patently egregious and unlawful behavior, was intentional and/or willful.

133. Each of Defendants TRICARE, DOD, and Secretary's Privacy Act violations proximately caused adverse effects to Plaintiffs and the Class.

134. Defendants TRICARE, DOD, and Secretary's failure to safeguard and prevent unauthorized disclosure of individuals' medical records, names, addresses and phone numbers linked to their Social Security numbers has, in particular, placed each Plaintiff and Class

Member in legitimate fear of imminent identity theft, corruption of his or her credit files, plundering of bank accounts and retirement funds, and have caused Plaintiffs and the Class to suffer actual damages, including unauthorized credit card charges and the purchasing of credit reports and credit monitoring services. Defendants TRICARE, DOD, and Secretary's actions have resulted in the disclosure of private personal information concerning each Plaintiff's health and medical care and have placed each Plaintiff and Class Member at imminent risk of medical identity theft.

135. Defendants TRICARE, DOD, and Secretary's failure to safeguard and prevent unauthorized disclosures caused adverse effects and actual damages to Plaintiffs and the Class. Plaintiffs and the Class are entitled to monetary relief, including statutory damages of $1,000, and the cost of this action, including reasonable costs and attorneys' fees.

Count 3: Willful and/or Negligent Violation of the FCRA Against Defendant SAIC

136. Plaintiffs incorporate by reference those paragraphs set forth above as if fully set forth herein.

137. The FCRA requires consumer reporting agencies to adopt and maintain procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy, and proper utilization of such information. 15 U.S.C. § 1681(b).

138. The FCRA defines a "consumer reporting agency" as:

> Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or

> facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

139. The FCRA defines a "consumer report" as:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes, employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b).

15 U.S.C. § 1681a(d)(1).

140. The FCRA defines "medical information" as:

> [I]nformation or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to – (A) the past, present, or future physical, mental, or behavioral health or condition of an individual; (B) the provision of health care to an individual; or (C) the payment for the provision of health care to an individual.

15 U.S.C. § 1681a(i).

141. The FCRA specifically protects medical information, restricting its dissemination to limited instances. *See, e.g.*, 15 U.S.C. §§ 1681a(d)(3), 1681b(g), 1681c(a)(6).

142. SAIC is a Consumer Reporting Agency as defined under FCRA because on a cooperative nonprofit basis and/or for monetary fees, SAIC regularly engages, in whole or in part, in the practice of assembling information on consumers for the purpose of furnishing Consumer Reports to third parties and/or uses interstate commerce for the purpose of preparing and/or furnishing Consumer Reports.

143. As a Consumer Reporting Agency, SAIC was (and continues to be) required to adopt and maintain procedures designed to protect and limit the dissemination of consumer credit, personnel, insurance, and other information (such as Plaintiff's and Class Members' private health information) in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy, and proper utilization of such information. SAIC, however, violated FCRA by failing to adopt and maintain such protective procedures which, in turn, directly and/or proximately resulted in the theft of the backup data tapes and wrongful dissemination of Plaintiff's and Class Members' private health information into the public domain.

144. Plaintiff's and Class Members' private health information, in whole or in part, constitutes medical information as defined under FCRA. SAIC also violated FCRA by failing to specifically protect and limit the dissemination of Plaintiff's and Class Members' private health information (*i.e.*, their medical information) into the public domain.

145. SAIC's repeated violations of FCRA, as set forth above, were willful or, at the very least, reckless or negligent.

146. As a direct and/or proximate result of SAIC's violations of FCRA, as described above, Plaintiff's and Class Members' private health information was disclosed and made accessible to unauthorized third parties in the public domain.

147. As a further direct and/or proximate result of SAIC's violations of FCRA, as described above, Plaintiff and the Class Members suffered actual damage 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. SAIC's wrongful actions and/or inaction violated FCRA.

148. Plaintiff and Class Members, therefore, are entitled to compensation for their actual damages or statutory damages of not less than $100, and not more than $1000, per Class Member, as well as attorneys' fees, litigation expenses, and costs, pursuant to 15 U.S.C §1681n(a).

Count 4: Breach of Third-Party Beneficiary Contract Against Defendant SAIC

149. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

150. SAIC contracts with TRICARE and DOD to protect and hold in its care sensitive personal information of Plaintiffs and the Class ("Care Contracts").

151. Under the circumstances and in recognition of a right to performance of the Care Contracts, SAIC, TRICARE, and DOD intended to give Plaintiffs and the Class the benefit of the performance promised by SAIC.

152. Pursuant to the Care Contracts, Plaintiffs and the Class are intended third party beneficiaries.

153. SAIC substantially breached the Care Contracts by, *inter alia*, failing to adequately safeguard Plaintiffs' and the Class' sensitive personal information. SAIC breached the Care Contracts by, *inter alia*, failing to monitor, audit, oversee, and confirm that SAIC's safeguards were adequate and complied with all applicable laws.

154. SAIC's breach of the Care Contracts directly and/or proximately caused Plaintiffs and the Class to suffer actual and substantial damages in the form of, *inter alia*, the costs of monitoring accounts for instances of fraud and the costs of additional safeguards to protect themselves from identity theft.

155. Plaintiffs are entitled to monetary relief including restitution, damages, and reasonable costs to mitigate damages as a result of SAIC's breach.

Count 5: Negligence
Against Defendant SAIC

156. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

157. Upon coming into possession of the private, non-public, sensitive financial information of Plaintiff and Class Members, SAIC had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the Confidential Information from being compromised and/or stolen. SAIC's duty arises from the common law, in part because it was reasonably foreseeable to SAIC that a breach of security was likely to occur under the circumstances and it would cause damages to the Plaintiffs and Class Members as alleged herein, as well as from the duties expressly imposed upon SAIC from other sources, such as expressed and implied contracts between SAIC and Class Members.

158. SAIC also had a duty to timely disclose to Plaintiffs and Class Members that the Security Breach occurred and the private, non-public, sensitive Confidential Information of Plaintiffs and the Class Members had been compromised. SAIC's duty to disclose the Security Breach to Plaintiffs and Class Members also arises from the above same sources.

159. SAIC also had a duty to put into place internal policies and procedures designed to protect Plaintiffs' and Class Members' private, non-public, sensitive Confidential Information that was within its possession, custody, and control.

160. SAIC, by and through its above negligent acts and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by, among other things, failing to exercise

reasonable care in protecting and safeguarding Plaintiffs' and Class Members' private, non-public, sensitive Confidential Information that was within its possession, custody, and control.

161. SAIC, by and through its above negligent acts and/or omissions, further breached its duties to Plaintiffs and Class Members by failing to put into place internal policies and procedures designed to protect and safeguard Plaintiffs' and Class Members' private, non-public, sensitive Confidential Information within its possession, custody, and control.

162. But for SAIC's negligent and wrongful breach of the duties it owed (and continues to owe) to Plaintiffs and Class Members, the Plaintiffs' and Class Members' private, non-public, sensitive Confidential Information would never have been wrongfully disseminated, the Security Breach would not have occurred and Plaintiffs and Class Members would not have been damaged.

163. SAIC's negligent and wrongful breach of the duties it owed (and continues to owe) to Plaintiffs and Class Members was the proximate cause of damages sustained by Plaintiffs and Class Members.

164. Having their personal and private information compromised damaged Plaintiffs, requiring Plaintiffs to take steps to ensure that they are not the victim of identity theft, credit card fraud, or other crimes.

165. The wrongful disclosure and the above-described injuries suffered by Plaintiffs and Class Members as a direct and/or proximate result of the security breach were reasonably foreseeable consequences of SAIC's negligence or gross negligence.

166. Plaintiffs are entitled to monetary relief including damages and reasonable costs to mitigate damages as a result of SAIC's negligence, as well as punitive damages.

Count 6: Violation of California Confidentiality of Medical Information Act, California Civil Code § 56 *et seq.* Against Defendant SAIC

167. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

168. California Civil Code section 56, *et seq.*, known as the Confidentiality of Medical Information Act, prohibits health care providers and contractors from disclosing medical information regarding a patient without first obtaining written authorization from a patient.

169. At all relevant times, SAIC was both a contractor and a health care provider under California law, because it had the "purpose of maintaining medical information in order to make the information available to the patient or to a provider of health care at the request of the patient or a provider of health care, for purposes of diagnosis or treatment of the patient." Cal. Civ. Code § 56.06(a).

170. At all relevant times, SAIC had a legal duty to protect the confidentiality of Plaintiffs and Class Members' medical information.

171. By disclosing the private medical information of Plaintiffs and the Class without written authorization, SAIC violated section 56, *et seq.* and its legal duty to protect the confidentiality of such information.

172. SAIC also violated Sections 56.06 and 56.101 of California's Confidentiality of Medical Information Act, which prohibits the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential medical information.

173. Pursuant to Section 56.36, Plaintiffs and Class Members are entitled to nominal statutory damages of $1,000 per class member.

Count 7: Violation of California Security Notification Requirements, Cal. Civil Code § 1798.20 *et seq.* and § 1798.80 *et seq.* Against Defendant SAIC, On Behalf Of The California Subclass

174. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

175. Defendant SAIC unreasonably delayed informing anyone about the breach of security for Plaintiffs' and Class Members' private and sensitive Confidential Information after Defendant SAIC knew such breach occurred.

176. Defendant SAIC failed to disclose to Plaintiffs and Class Members in the most expedient time possible and without unreasonable delay, the breach in security of Plaintiffs' unencrypted private and sensitive Confidential Information when SAIC knew or reasonably believed such information has been acquired by unauthorized persons.

177. Plaintiffs and Class Members are indirect customers of SAIC.

178. No law enforcement agency determined or instructed Defendant SAIC that notification of the breach would impede any criminal investigation.

179. As a direct and proximate result of Defendant SAIC's actions and omissions described herein, Plaintiffs and Class Members have suffered damages.

180. Plaintiffs Mrs. Hartman and the California subclass are entitled to monetary relief including statutory damages and injunctive relief as a result of SAIC's actions and omissions.

Count 8: Violation of the D.C. Consumer Security Breach Notification Statute D.C. Code §28-3851 *et. seq.* Against Defendant SAIC, On Behalf Of The D.C. Subclass

181. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

182. SAIC's actions, taken in the course of SAIC's trade, violated numerous laws of the District of Columbia, including the D.C. Consumer Security Breach Notification Statute. D.C. Code § 28-3852.

183. SAIC caused unknown and unauthorized individuals to acquire confidential computerized or other electronic data. This acquisition compromised the security, confidentiality, and integrity of personal information relating to the D.C. Class.

184. In contravention of the D.C. Consumer Security Breach Notification Statute, SAIC failed to notify victims of the breach in the most expedient time possible.

185. In further contravention of the D.C. Consumer Security Breach Notification Statute, SAIC failed to promptly give notice of the disclosure to all consumer reporting agencies that compile and maintain files.

Count 9: Violation of the D.C. Consumer Protection Procedures Act
D.C. Code §28-3901 *et. seq*.
Against Defendant SAIC

186. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

187. SAIC's actions, taken in the course of SAIC's trade, violated numerous laws of the District of Columbia.

188. SAIC's actions also violate D.C. Code § 28-3904(a) and (d) in that SAIC has represented to Plaintiffs and Class Members that its service has a certain characteristic or quality, namely the security of their private and confidential information when, as alleged herein, SAIC routinely fails to follow corporate or industry standards in maintaining the safety and security of such information.

189. SAIC also misrepresented a material fact in violation of §28-3904(e) when it vaguely informed the public that the risk of fraud and identity theft was low. Given the high risk of fraud and identity theft, and SAIC's subsequent offer of (insufficient) credit monitoring plan, SAIC's misrepresentations had a tendency to mislead consumers.

190. Furthermore, SAIC advertised its services without the intent to sell them as advertised in violation of §28-3904(h). Namely, SAIC advertised and promised its consumers that it would comply with industry and corporate policies regarding the security and safeguarding of the sensitive and private information when it did not.

191. Class Members were accordingly injured by SAIC's violations of D.C. law. As such, they are entitled to: (a) treble damages, or $1,500 per violation, whichever is greater, payable to the consumer; (b) reasonable attorney's fees; (c) punitive damages; (d) an injunction against the use of the unlawful trade practice; (e) additional relief as may be necessary to restore to the consumer money or property, real or personal, which may have been acquired by means of the unlawful trade practice; and (f) any other relief which the court deems proper.

Count 10: Violation of the D.C. Consumer Protection Procedures Act
D.C. Code §28-3901 *et. seq*.
Against Defendant SAIC, on Behalf of the General Public

192. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

193. Defendant SAIC made false representations throughout the District of Columbia. Defendant caused damage and adverse effects to residents of this District.

194. Plaintiffs act for the benefit of the General Public as a Private Attorney General pursuant to District of Columbia Code §28-3905(k)(1).

195. SAIC's actions, taken in the course of SAIC's trade, violated numerous laws of the District of Columbia, including the D.C. Consumer Security Breach Notification Statute. D.C. Code § 28-3852.

196. SAIC's actions also violate D.C. Code § 28-3904(a) and (d) in that SAIC has represented to Plaintiffs and the General Public that its service has a certain characteristic or quality, namely the security of their private and confidential information when, as alleged herein, SAIC routinely fails to follow corporate or industry standards in maintaining the safety and security of such information.

197. SAIC also misrepresented a material fact in violation of §28-3904(e) when it vaguely informed the public that the risk of fraud and identity theft was low. Given the high risk of fraud and identity theft, and SAIC's subsequent offer of (insufficient) credit monitoring plan, SAIC's misrepresentations had a tendency to mislead consumers.

198. Furthermore, SAIC advertised its services without the intent to sell them as advertised in violation of §28-3904(h). Namely, SAIC advertised and promised its consumers that it would comply with industry and corporate policies regarding the security and safeguarding of the sensitive and private information when it did not.

199. The general public was accordingly injured by SAIC's violations of D.C. law. As such, it is entitled to: (a) treble damages, or $1,500 per violation, whichever is greater; (b) reasonable attorney's fees; (c) punitive damages; (d) an injunction against the use of the unlawful trade practice; (e) additional relief as may be necessary to restore to the consumer money or property, real or personal, which may have been acquired by means of the unlawful trade practice; and (f) any other relief which the court deems proper. §28-3905(k)(1).

Count 11: Violation of Security Breach Notification Statutes Against Defendant SAIC, On Behalf Of The Multistate Subclass

200. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

201. SAIC caused unknown and unauthorized individuals to acquire confidential computerized or other electronic data. This acquisition compromised the security, confidentiality, and integrity of personal information relating to Plaintiffs and Class Members.

202. In contravention of numerous state statutes, SAIC failed to notify victims of the breach in the most expedient time possible.[2]

Count 12: Declaratory Relief Pursuant to 28 U.S.C. § 2201 *et seq.* Against Defendants TRICARE, DOD, Secretary, and SAIC

203. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

204. An actual, justiciable controversy, over which this Court has jurisdiction, has arisen and now exists between the parties relating to the legal rights and duties of Plaintiffs and Defendants for which Plaintiffs desire a declaration of rights. This controversy is of sufficient immediacy and reality to warrant the issuance of a declaratory judgment pursuant to 28 U.S.C. § 2201.

[2] Numerous States maintain the same requirement that the existence of a security breach be disclosed "in the most expeditious time possible" and/or "without unreasonable delay" and provide for damages recoverable in civil suits for violations. *See, e.g.*, Alaska Stat. § 45.48.010 *et seq.*; Cal. Civ. Code § 56 *et seq.*; Conn. Gen Stat 36a-701b *et. seq.*; Haw. Rev. Stat. § 487N-2 *et. seq.*; 850 ILCS 550/1 *et. seq.* (Illinois); Iowa Code § 715C.1 *et seq.*; La. Rev. Stat. § 51:3071 *et. seq.*; Md. Code. Com. Laws § 14-3501 et. seq.; N.H. Rev. Stat. § 359-C:19 *et. seq.*; N.C. Gen. Stat. §75-65 *et. seq.*; R.I. Gen. Laws § 11-49.2-1 et. seq.; S.C. code § 39-1-90 *et. seq.*; Wash. Rev. Code § 19.255.010 *et. seq.* Accordingly, such claims are brought on behalf of the Multistate subclass, which includes Class Members in all states with such laws.

205. A declaratory judgment is necessary to determine Plaintiffs' rights in connection with Defendants' maintenance of Plaintiffs' private and sensitive Confidential Information.

206. Plaintiffs seek a declaratory judgment that Defendants, collectively or individually, violated the APA, the Privacy Act, the FCRA, the California Confidentiality of Medical Information Act, the D.C. Consumer Protection Procedures Act, and the Notification Laws of California, D.C. and various other states. Plaintiffs also seek a declaratory judgment that Plaintiffs are intended third party beneficiaries to the Care Contracts between the Defendants.

PRAYER FOR RELIEF

WHEREFORE, the Plaintiffs, individually and on behalf of the Class Members, respectfully request that (a) Defendants be required to appear and answer this lawsuit, (b) this action be certified as a class action, (c) Plaintiffs be designated the Class Representatives, and (d) Plaintiffs' Counsel be appointed as Class Counsel. Plaintiffs, individually and on behalf of the Class Members, further request that upon final trial or hearing, judgment be awarded against Defendants for:

(i) actual damages to be determined by the trier of fact;

(ii) statutory damages, punitive damages, and treble damages;

(iii) pre- and post-judgment interest at the highest legal rates applicable;

(iii) appropriate injunctive and/or declaratory relief, including injunctive relief requiring Defendants to comply with their obligations to monitor, audit, oversee and confirm that their procedures and safeguards are adequate and comply with all applicable laws and guidance are in place and being properly managed, updated and maintained to minimize the likelihood of future data breaches;

(v) reasonable attorneys' fees and litigation expenses incurred through the trial and any appeals of this case;

(vi) costs of suit; and

(vii) such other and further relief that this Court deems just and proper.

Dated: February 21, 2012

Respectfully submitted,

/s/ James R. Denlea
James R. Denlea
Jeffrey I. Carton
Jeremiah Frei-Pearson
MEISELMAN, DENLEA, PACKMAN, CARTON & EBERZ, P.C.
1311 Mamaroneck Avenue
White Plains, NY 10605
Telephone: (914) 517-5000
Facsimile: (914) 517-5055
jdenlea@mdpcelaw.com
jcarton@mdpcelaw.com
jfrei-pearson@mdpcelaw.com

/s/ Tracy D. Rezvani
Tracy D. Rezvani
Mila Bartos
Rosalee B. C. Thomas
FINKELSTEIN THOMPSON LLP
1077 30th Street, N.W.
Suite 150
Washington, D.C. 20007
Telephone: (202) 337-8000
Fax: (202) 337-8090
trezvani@finkelsteinthompson.com
mbartos@finkelsteinthompson.com
rbcthomas@finkelsteinthompson.com

/s/ Andrew N. Friedman
Andrew N. Friedman
Agnieszka Fryszman
Stefanie M. Ramirez
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue NW
Suite 500 West
Washington, DC 20005
Telephone: (202) 408-4600
Fax: (202) 408-4699

afriedman@cohenmilstein.com
afryszman@cohenmilstein.com
sramirez@cohenmilstein.com