UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JAMES F. BIGGERMAN JR.,
1233 Stonehedge Way
Shelbyville, IN 46176

on behalf of himself and all others similarly situated,

Plaintiff,

vs.

TRICARE MANAGEMENT ACTIVITY,
Skyline 5, Suite 810
5111 Leesburg Pike
Falls Church, VA 22041-3206

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION,
1710 SAIC Drive
McLean, VA 22102

UNITED STATES DEPARTMENT OF DEFENSE,
1400 Defense Pentagon
Washington, D.C. 20301-1400

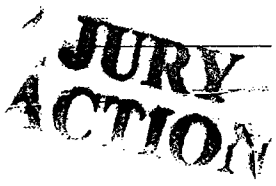
and

LEON E. PANETTA, in his Official Capacity as Secretary of Department of Defense,
1400 Defense Pentagon
Washington, D.C. 20301-1400

Defendants.

Civil Action No.:

JURY TRIAL DEMANDED



Case: 1:11-cv-02142
Assigned To : Wilkins, Robert L.
Assign. Date : 12/1/2011
Description: FOIA/Privacy Act

CLASS ACTION COMPLAINT

Plaintiff, James F. Biggerman Jr., on behalf of himself and all others similarly situated, brings this class action suit against Defendant TRICARE Management Activity ("TMA"), the

agency administering the TRICARE health care program ("TRICARE") to uniformed service members, retirees and their families, Science Applications International Corporation ("SAIC"), the United States Department of Defense ("DOD"); and Leon Panetta, in his Official Capacity as Secretary of DOD ("Secretary of DOD") (collectively, "Defendants"). Plaintiff alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action suit on his own behalf and on behalf of all persons similarly situated against Defendants, as a result of Defendants' failure to adequately safeguard their millions of military clinic and hospital patients' personally identifiable and protected health information (hereinafter "Confidential Information"). Such Confidential Information includes members' Social Security numbers, addresses, phone numbers, and some personal health data such as clinical notes, laboratory tests, and prescription information.

2. As a result of Defendants' failure to adequately protect and secure Plaintiff's and Class members' Confidential Information, unauthorized individuals gained access to Plaintiff's and Class members' Confidential Information (the "Confidential Information Theft").

3. Defendants' failure to maintain reasonable and adequate security procedures to protect against the theft of Plaintiff's and other Class members' Confidential Information has put them at an increased risk of becoming victims of identity theft crimes, fraud, abuse, and extortion, including out of pocket costs to protect themselves from identity theft in the future.

4. Plaintiff and other members of the Class will suffer irreversible damage if their Confidential Information becomes public. As a proximate result of the Confidential Information Theft, 4.9 million TRICARE members, including Plaintiff, have had their Confidential Information compromised, their privacy invaded, have been deprived of the exclusive use and

control of their proprietary prescription information, have incurred costs of time and money to consistently monitor their credit card accounts, credit reports, prescription accounts, and other financial information in order to protect their Confidential Information, and have otherwise suffered economic damages.

JURISDICTION & VENUE

5. 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. 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.

6. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because at least one member of the class is a citizen of a different state that Defendants; there are more than 100 putative Class members nationwide; and the aggregate amount in controversy exceeds $5,000,000. This Court has personal jurisdiction over the parties because the DOD and the Secretary of DOD have their principal place of business in this district and conduct substantial business in this state, have systematic and continuous contacts with this district, and have agents and representatives that can be found in this district. Defendants TMA and SAIC are authorized to do business and in fact do business in the District of Columbia, and Defendants TMA and SAIC have sufficient minimum contacts with the District of Columbia and otherwise intentionally avail themselves of the markets in the District of Columbia to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

7. Pursuant to 28 U.S.C § 1391(a)(2), venue is proper in the District Court for the District of Columbia because the DOD and the Secretary of the DOD are headquartered in the

District of Columbia. Venue is also proper in the District Court for the District of Columbia pursuant to 5 U.S.C. §§ 552a(g)(5).

PARTIES

8. Plaintiff James Biggerman is a resident of Shelbyville, Indiana. Mr. Biggerman is a retired Commander Sergeant Major with the Army. Defendants possess Plaintiff's highly sensitive personal and medical information, which, pursuant to federal law, Defendants are required to keep confidential. As a result of Defendants' unlawful conduct, Plaintiff's ~~Confidential Information has been exposed, putting him at risk of identity theft.~~

9. Defendant TMA is headquartered at Skyline 5, Suite 810, 5111 Leesburg Pike, Falls Church, VA 22041-3206. TMA was established under the DOD to manage the TRICARE health care program for active duty members and their families, retired service members and their families, National Guard/Reserve members and their families, survivors and others entitled to DOD medical care. TMA is within the Military Health System ("MHS"), the fully integrated healthcare system of the DOD, and is considered an "agency" under the Federal Privacy Act, 5 U.S.C. § 552a *et seq.*

10. Defendant SAIC is a Delaware corporation headquartered at 1710 SAIC Drive, McLean, Virginia 22102. SAIC is a leading government services contractor and provides a wide range of information technology services, including systems engineering and project management, to federal and state agencies, including the DOD. As a government contractor of DOD, SAIC, is considered an "agency" under the Federal Privacy Act, 5 U.S.C. § 552a *et seq.*

11. Defendant DOD is a government agency headquartered at 1400 Defense Pentagon, Washington, D.C. 20301-1400. DOD provides the military forces that protect the security of the United States. The DOD is considered an "agency" under the Private Act.

12. Defendant Leon E. Panetta ("Secretary"), in his Official Capacity as Secretary of the DOD is located at 1400 Defense Pentagon, Washington, D.C. 20301-1400. The Secretary is responsible for the formulation of general defense policy and policy related to all matters of direct concern to the Department of Defense, and for the execution of approved policy.

FACTUAL BACKGROUND

13. Since February 1998, Defendant TMA has managed the TRICARE health care program for active duty members and their families, retired service members and their families, ~~National Guard/Reserve members and their families, survivors and others entitled to DOD~~ medical care. Thus, the TMA and DOD are responsible for protecting private personal information for millions of military service people and their families. TMA and DOD are legally required to maintain the privacy of this Confidential Information.

14. With these duties to ensure the privacy of TRICARE members' Confidential Information, TMA and the DOD are also responsible for hiring and contracting with those who will do the same.

15. TMA and DOD hired SAIC as a government contractor to transport the Confidential Information received by TMA and the DOD. As a government contractor for TMA and the DOD, SAIC also had the duty to ensure the privacy of the TRICARE members' Confidential Information. *See* Privacy Act of 1974, 5 U.S.C. §552(a)(m)(1).

16. Although Defendants are entrusted with such Confidential Information and have a duty to protect this information, Defendants have continuously failed to maintain reasonable and adequate security procedures to protect against the theft of Plaintiff's and other members of the Class members' Confidential Information.

17. For example, on July 23, 2007, TMA announced a potential compromise of personal information belonging to TRICARE beneficiaries. According to that announcement:

> A limited amount of TRICARE beneficiary data may have been placed at risk through a violation of internal IT security practices at Science Applications International Corporation (SAIC). The potential compromise occurred when patient data was stored in a manner that did not meet stringent security specifications for the Department of Defense or SAIC. This information may consist of combinations of name, sponsor, Social Security Number, family member prefix, address and/or date of birth in combination with medical appointment and/or health information, mostly in the form of codes that represent medical diagnosis and procedures. The information was held on a single, SAIC-owned server at an SAIC location in Florida. The server, which was not behind a firewall and did not contain adequate password protections, is no longer in use.

18. With knowledge of previous privacy breaches and SAIC's alleged wrongdoings, TMA, DOD, and the Secretary failed to take precautionary measures to ensure the privacy of TRICARE members.

19. On September 14, 2011, SAIC reported a data breach involving personally identifiable and protected health information impacting an estimated 4.9 million military clinic and hospital patients served by TRICARE.

20. The Confidential Information was contained on improperly encrypted or unencrypted computer backup tapes from an electronic health care record use in the MHS to capture patient data from 1992 through September 7, 2011.

21. The Confidential Information includes Social Security numbers, addresses and phone numbers, and personal health data such as clinical notes, laboratory tests, prescriptions, diagnosis, treatment information, provider names, provider locations and other patient data.

22. The Confidential Information was stolen from an SAIC employee's vehicle in San Antonio, Texas. SAIC is a company contracted by the TMA and the DOD to assist with the

management of TRICARE members' Confidential Information. SAIC was contracted to transport the TRICARE Confidential Information.

23. SAIC admitted that the Confidential Information was not properly encrypted—contrary to applicable standards. Vernon Guidry, an SAIC spokesman, said in a statement that "the operating system used by the government facility to perform the backup onto the tape was not capable of encrypting data in a manner that was compliant with the relevant federal standard."

24. Guidry also added that he was surprised that a computer tape containing millions of health records was left in an SAIC employee's vehicle for an entire work day. Guidry said he would suggest using an armored car to transport such a large amount of sensitive data.

25. The SAIC employee from whose car Plaintiff's personal information was stolen did not receive a security background check nor did he receive the requisite trainings mandated by federal law.

26. Although Defendants were made aware of the Confidential Information Theft on or about September 14, 2011, Defendants did not inform the public and TRICARE members until on or about September 29, 2011, more than two weeks later.

27. On or about September 29, 2011, TRICARE issued a press release and stated on its website that individual notifications would be issued "within the next 6 weeks" as to whether their individual information was on the tapes.

28. Defendants' mere explanation for the delay in notification was "this data loss remains the subject of an ongoing investigation... We did not want to raise undue alarm in our beneficiaries and so wanted to determine the degree of risk this data loss represented before making notifications."

29. According to TRICARE Operations Manual of February 1, 2008, "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."

30. Defendants' response to breach is insufficient and fails to comply with the procedures required by law. Defendants' informational website hardly describes the breach of Confidential Information, and gives little detail to its members as to whether their information was affected. Defendants have not acted in accordance with its obligations to protect its members' Confidential Information. Defendants should have: 1) prevented a breach of this magnitude from occurring in the first instance and 2) provided individual notice to its affected customers as soon as it discovered the breach.

31. Defendants also fail to explain why the company stored members' Confidential Information in such an improperly secured manner.

32. Defendants' repeated failures to correct known vulnerabilities of DOD's safeguards for Plaintiff's private information demonstrate a reckless disregard for TRICARE members' privacy and rights and intentional or willful violations of the Privacy Act.

33. 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.

34. Due to the dangers of identity theft, federal and state legislatures have passed laws to ensure companies protect the security of sensitive personally identifiable information in the company's files. *See* The President's Identity Theft Force Report (Sept. 2008) available at:

http://www.ftc.gov/os/2008/10/081021taskforcereport.pdf at 13. These laws include requirements for the handling of personally identifiable information by financial institutions.

35. The Federal Trade Commission ("FTC") has issued a publication entitled "Protecting Personal Information: A Guide for Business" ("FTC Report"). In this publication, the FTC 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 personally identifiable 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 personally identifiable 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 indentifying information.

36. 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.

37. Plaintiff and class members are now at risk of becoming victims of such a crime as a result of Defendants' conduct.

38. Many of these laws include requirements for the handling of Confidential Information by health care providers, and also impose proactive obligations on companies to maintain reasonable security measures to protect and individual's Confidential Information.

39. Defendants must protect the TRICARE members' sensitive personal information, and Defendants must also meet the requirements of Health Insurance Portability and Accountability Act ("HIPAA"). HIPAA sets strict guidelines to protect individually identifiable health information, and protect medical records of all kinds –paper and, especially, electronic— with the most sophisticated kinds of security systems available, including backup protections and automatic alerts of security violations.

40. HIPAA created national standards for transmitting electronic health care transactions, protecting patient privacy, and ensuring the security of individually identifiable health information. The Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") establishes standards to protect individually identifiable health information, including restricting disclosures of protected health information to the minimum necessary for the intended purpose.

41. HIPAA also enacted security standards for protecting information, including: administrative safeguards to execute security measures to protect data and manage the conduct of personnel in relation to the protection of data; physical safeguards, including the protection of physical computer systems and the buildings holding such systems from inappropriate intrusion or removal; and technical safeguards to protect information, authenticate users, and control individual access to information.

42. Defendants have pledged their compliance with these federally mandated standards.

43. In marketing its services to TRICARE members, Defendants have promised to maintain the privacy of members' CONFIDENTIAL INFORMATION pursuant to its obligations under federal law as enacted by HIPAA. *See* TMA's Privacy and Civil Liberties Office notice, *available at* http://www.tricare.mil/tma/privacy/.

44. TMA promises to be compliant with all the applicable mandates of HIPAA, including but not limited to the following privacy specific provisions:

a. Ensuring that DOD Health Affairs (HA) and TMA policies and business practices comply with federal laws, DOD regulations, and guidelines governing the privacy and security of CONFIDENTIAL INFORMATION, and in the development and revision of TMA privacy-related plans, policies, and procedures.

b. Managing and evaluating potential risks and threats to the privacy and security of MHS health data by performing critical reviews through:

   i. Evaluation of privacy and security safeguards, including conducting annual Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Risk Assessments

   ii. Performance of Internal Privacy Office Compliance Assessments

   iii. Establishment of organizational performance metrics to identify and measure potential compliance risks

c. Engaging TMA stakeholders, including employees and contractors, by developing and delivering education and awareness materials and ongoing workforce privacy and HIPAA security training

45. SAIC ensures compliance with all the applicable mandates of HIPAA and other laws and regulations:

> Our team of security specialists has deep knowledge and understanding of the Health Insurance Portability and Accountability Act (HIPAA) security and privacy rules and the Federal Information Security Management Act (FISMA), as well as other applicable federal laws and regulations. Our security and privacy experts not only help our customers comply with legal mandates, but also help assure that our information technology solutions will effectively protect the confidentiality of sensitive information, the integrity of critical data, and the availability of necessary services....

52. Members' Confidential Information includes names, dates of birth, Social Security numbers, and corresponding prescription information. Such information is a property interest owned by TRICARE's members and is not owned by Defendants.

53. Members trust Defendants to protect their Confidential Information for the limited purpose of providing medical benefits. Members expect that their Confidential Information will not be disclosed except under limited and appropriate circumstances. Those circumstances are limited to processing health insurance and similar payment requirements, public health emergencies, and/or other narrow uses specified under HIPAA.

54. Defendants exercise discretionary authority and control over the administration and management of the plans, including how to secure its members' Confidential Information and the limited circumstances under which disclosure of Confidential Information is permitted under HIPAA.

55. Defendant Secretary was ultimately responsible for control, direction, and management of the DOD's processes, policies, and procedures for compliance with the Privacy Act, 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 Plaintiff's privacy rights, but failed to ensure correction or mitigation of those deficiencies.

56. Defendant Secretary flagrantly disregarded Plaintiff's privacy rights and harmed Plaintiff and class members by failing to establish and ensure lawful compliance by his subordinates 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 results in substantial harm to any individual whose information was maintained.

57. Defendants are obligated to discharge their duties for the exclusive purpose of providing benefits to participants and beneficiaries, and defraying reasonable expenses of administering the plans. Defendants are also obligated to act with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims.

58. Upon information and belief, Defendants failed to follow reasonable precautions to secure its members' Confidential Information, failed to provide timely notice, and failed protect its members from invasion of privacy, fraud, and identity theft.

59. As defined in the Fair and Accurate Credit Transactions Act of 2003, Pub.L. 108-159, Dec. 4, 2003 (FACTA), "identity theft" is a fraud that is committed or attempted when one person is using another person's identifying information without permission. 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. The FTC has stated that identity theft has been a serious problem in recent years, with approximately 9 million Americans falling victim to identity theft each year.

60. As the United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report"), more than 570 breaches involving theft of personal identifiers such as Social Security numbers were reported by the news media from January 2005 through January 2006. *See* http://www.gao.gov/new.items/d07737.pdf. These data breaches involve the "unauthorized or unintentional exposure, disclosure, or loss of sensitive Confidential

Information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers."

61. The GAO Report 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.

62. 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 personally identifiable information, Social Security Numbers are even more difficult to change and their misuse can continue for years into the future.

63. Furthermore, 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.

64. In a pamphlet called "identity Theft Repair Kit," the Office of the Attorney General of Colorado, John W. Suthers, outlines the immediate consequences of such a breach. An identity thief can then open a new credit card with the delinquent account reported on the victim's credit report. The imposter changes the mailing address on the victim's credit card account so that it will take some time before the victim realizes that there is a problem. The thief can establish phone or wireless service in the victim's name or open a bank account and use it to write bad checks. The thief can also file for bankruptcy to avoid paying debts or to avoid eviction. If arrested, the thief can give the police the victim's name, affecting their criminal record and subjecting the victim to arrest for not appearing in court. The thief can also make

purchases related to illegal activities or take out an auto loan. *See* http://www.coloradoattorneygeneral.gov/sites/default/files/uploads/identity_theft/idtrk.pdf.

65. Identity theft crimes often include more than just crimes of financial loss. Identity thieves also commit various types of government fraud, such as: obtaining a driver's license or official identification card in the victim's name but with their picture; using the victims name and Social Security number to obtain government benefits; or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or get medical services in the victim's name, and may even give the victim's Confidential Information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

66. Victims of identity theft often have a great deal of difficulty clearing their credit records, which can significantly impair their credit rating and ability to obtain loans. While law enforcement, banks, credit bureaus, and collection agencies all have procedures to help identity theft victims, it can still take weeks, months, or years of effort and frustration to return to normal. A damaged credit history can also cause difficulty for the victim in obtaining a new job or renting an apartment, as employers and landlords often review credit records of new applicants. *Id.*

67. Identity theft victims spend numerous hours and money repairing damage to their good name and credit records. In addition, a person whose Confidential Information has been compromised may not see any signs of identity theft for years. According to the United States GAO which conducted a comprehensive and extensive study of data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that

> information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See http://www.gao.gov/new.items/d07737.pdf.

68. Defendants' failures alleged herein caused Plaintiff adverse effects including, but not limited to, mental distress, emotional trauma, inconvenience, loss of peace of mind, embarrassment, pecuniary damages and the threat of current and future harm from identify theft.

69. The real threat of identity theft and similar adverse effects of the Defendants' unlawful actions and the inactions requires affirmative actions by Plaintiff to recover peace of mind, emotional stability, and personal security, including, but not limited to: purchasing credit reporting services; frequently obtaining and reviewing credit reports, bank statements and other similar information; and, closing or modifying financial accounts. Plaintiff has, and will continue to, suffer tangible and intangible damages for the foreseeable future.

70. Plaintiff and other members of the Class now face years of constant surveillance, and monitoring to prevent further loss and damage.

CLASS ACTION ALLEGATIONS

71. Pursuant to Rule 23(a) and (b)(1)-(3) of the Federal Rules of Civil Procedure, Plaintiff brings this class action on behalf of themselves and all other persons similarly situated who are TRICARE members and whose Confidential Information was compromised as a result of the Confidential Information Theft (the "Class"). The Class does not include Defendants, their officers, directors, agents, or employees.

72. The class is so numerous that joinder of all members is impracticable. The Class is compromised of approximately 4.9 million TRICARE members, which is the number of individuals whose information Defendants admit was collected and maintained in records which

were breached. Disposition of the claims as a class action will provide substantial benefits to both the parties and the Court.

73. The rights of each member of the Class were violated in a similar fashion based upon Defendants' uniform wrongful conduct.

74. Defendants' conduct affected all Class members in the same manner. Defendants' failure to properly safeguard Class members' Confidential Information and failure to notify Class members of the Confidential Information Theft as soon as practical after the breach was discovered affected Plaintiff and the other members of the Class in a uniform manner.

75. Common questions of fact and law exist as to all members of the Class and predominate over any questions affecting solely individual Class members. Among the questions of fact and law that predominate over individual issues are:

a. Whether Defendants breached their duties to Plaintiff and other members of the Class by failing to secure the Confidential Information of their members in violation of the Privacy Act;
b. Whether Defendants took reasonable steps and measures to safeguard Plaintiff's and other class members' Confidential Information;
c. Whether Defendants acted wrongfully by failing to properly safeguard their members' Confidential Information;
d. Whether Defendants failed to notify Plaintiff and other members of the Class of the Confidential Information Theft as soon as practical after the Confidential Information Theft was discovered; and
e. Whether Defendants breached their duty to exercise reasonable care in storing Plaintiff's and other members of the Class' Confidential Information by improperly securing that information on its computer network.

76. Plaintiff's claims are typical of the claims of the other members of the Class they seek to represent, because Plaintiff's Confidential Information like the Confidential Information of all members of the Class, was not adequately or reasonably secured by Defendants.

77. Plaintiff will fairly and adequately represent and protect the interests of the Class, in that he has no interest that is antagonistic to or that irreconcilably conflicts with those of other members of the Class.

78. Plaintiff has retained counsel competent and experienced in the prosecution of class action litigation.

79. This class action is fair and efficient and is the superior method of adjudicating the claims of Plaintiff and the Class members for the following reasons:

a. Common questions of law and face predominate over any question affecting any individual Class member;
b. The prosecution of separate actions by individual members of the Class would likely create a risk of inconsistent or varying adjudications with respect to individual members of the Class, thereby establishing incompatible standards of conduct for Defendants or would allow some Class members' claims to adversely affect other Class members' ability to protect their interests;
c. This forum is appropriate for litigation of this action because the cause of action arose in this District;
d. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and
e. The Class is readily definable, and prosecution as a class action will eliminate the possibility of repetitious litigation, while also providing redress for claims that may be too small to support the expense of individual, complex litigation.

FIRST CLAIM FOR RELIEF

Violation of the Privacy Act of 1974, 5 U.S.C § 552a *et seq.*

80. Plaintiff reasserts the allegations set forth in the preceding paragraphs and incorporates them by reference into this First Claim for Relief.

81. All Defendants violated the Privacy Act.

82. Each of Defendants' violations of the Privacy Act was intentional and/or willful.

83. Each of Defendants' Privacy Act violations caused Plaintiff's adverse effects.

84. Defendants' unauthorized disclosure of individuals' medical records, names, addresses, and phone numbers linked to their Social Security numbers has, in particular, placed Plaintiff in legitimate fear of identity theft and corruption of their credit files. Further, Defendants' practices have increased Plaintiff and the other members of the Class risk of being victims of identity theft and other harm. It has also resulted in the disclosure of private personal information concerning Plaintiff's health and medical care.

85. Plaintiff suffered actual damages as a result of Defendants' Privacy violations.

86. Plaintiff is entitled to monetary relief and the costs of this action, together with reasonable costs and attorneys fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all other persons similarly situated, respectfully requests that the Court enter an Order:

a. Certifying the proposed nationwide Class herein under Federal Rule of Civil Procedure 23(a) and (b)(1)-(3) and appointing Plaintiff as Class representative, and Plaintiff's counsel as Class counsel;
b. That this Court order Defendant Secretary to immediately identify in the Federal Register the existence and character of every system of records maintained by the DOD and make available to any individual therein, their authorized

representatives, or survivors, each record maintained in any DOD system of records pertaining to that individual.

c. That this court permanently enjoin Defendants, its officers, agents, employees and those acting for and with them, from accessing, viewing, handling, disclosing, or in any way transferring any record or system of records subject to the Privacy Act of 1974 requirements until an independent panel of experts finds that adequate information security has been established and implemented by the Defendants, unless such activity is explicitly allowed by Court order and under supervision of persons independent of Defendants, such supervision to be at Defendants' expense;

d. That this Court enjoin Defendants, its officers, agents, employees, and those acting for and with them from removing any device capable of storing, containing, or transferring any record or system of records, including but not limited to, laptop computers, portable hard drives, memory stick or similar devices, and "iPods" and similar devices, from property under Defendants' supervision and control until and unless Defendants demonstrate that adequate information security has been established to the Court's satisfaction.

e. Awarding other injunctive relief, including but not limited to: (i) the provision of credit monitoring and/or credit card monitoring services for the Plaintiff and other members of the Class; (ii) the provision of bank monitoring and/or bank monitoring services for the Plaintiff and the other members of the Class; (iii) the provisions of identity theft insurance for the Plaintiff and the other members of the Class; (iv) the requirement that Defendants receive periodic compliance audits by a third party regarding the security of its computer systems used for processing and storing customer data is in compliance with federal and industry rules and regulations, including but not limited to the mandates under HIPAA; and (v) the requirement that Defendant notify all members affected by the Confidential Information Theft.

f. That this Court grant Plaintiff's judgment against Defendants for damages in an amount of $1,000.00 for each individual who was adversely affected by Defendants'' Privacy Act violations;

g. Awarding all costs, and expenses, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

h. Providing for other legal and/or equitable relief as is permitted at law and as justice requires.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: December 1, 2011

Respectfully Submitted,

Andrew N. Friedman, #375595
Agnieszka M. Fryszman, #459208
Whitney R. Case, #501296
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, NW
Suite 500 West
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699

Irwin B. Levin
Richard E. Shevitz
Lynn A. Toops
COHEN & MALAD, LLP
One Indiana Square, Ste. 1400
Indianapolis, IN 46204
Telephone: (317) 636-6481
Facsimile: (317) 636-2593

Robert T. Thopy
MCNEELY, STEPHENSON, THOPY, & HARROLD
2150 Intelliplex Dr., Suite 100
Telephone: (317) 825-5110
Facsimile: (317) 825-5109