UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

CORNEILUS ALLISON, on behalf of himself and all others similarly situated,	Civil Action No._____
Plaintiff,	COMPLAINT – CLASS ACTION
v.	JURY TRIAL DEMANDED
AETNA, INC.	
Defendant.	

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff Corneilus Allison ("Plaintiff") hereby brings this class action suit against Aetna, Inc. ("Aetna" or the "Company"). Plaintiff makes the following allegations, except as to allegations specifically pertaining to Plaintiff and Plaintiff's counsel, based upon the investigation undertaken by Plaintiff's counsel, which included, *inter alia*, review and analysis of Defendant's website and various news articles. In support of Plaintiff's Class Action Complaint, Plaintiff alleges as follows:

JURISDICTION & VENUE

1. 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 some Class members are of diverse citizenship from the Defendant; there are more than 100 Class members nationwide; and the aggregate amount in controversy exceeds $5,000,000. This Court has personal jurisdiction over the parties because Defendant is incorporated in Pennsylvania, maintains offices in this state, and conducts business in this state.

2. Pursuant to 28 U.S.C. § 1391(a)(2), venue is proper in the Eastern District of Pennsylvania because a substantial part of the acts giving rise to Plaintiff's claims, such as the transactions by which Defendant became privy to Plaintiff's Sensitive Information (as hereinafter defined), occurred in this District.

NATURE OF ACTION

3. This is a class action lawsuit brought on behalf of Plaintiff, and on behalf of a class of all other persons similarly situated, against Aetna, Inc. for its failure to adequately protect the private personal information of its current, former, and potential employees, including but not limited to their names, Social Security numbers, home and/or office addresses, email addresses, telephone numbers, employment histories, and other information ("Sensitive Information").

4. Such persons were required to input their Sensitive Information into Aetna's website when they applied for a job with Aetna. Aetna also stored current and former employees' Sensitive Information on its website.

5. Defendant Aetna unlawfully failed to maintain reasonable systems and procedures

to protect Plaintiff's and the Class' Sensitive Information. As reported on May 27, 2009, as a result of Aetna's inadequate data security system, Aetna's website was hacked into by unknown third parties, and Plaintiff's and Class members' Sensitive Information was accessed and/or misused by unauthorized persons.

6. The website reportedly contained Sensitive Information of over 450,000 persons.

7. Plaintiff seeks damages suffered as a result of Defendant's practices, including but not limited to compensatory damages and injunctive relief.

PARTIES

8. Plaintiff Allison is a resident of Darby, Pennsylvania. As described further below, Plaintiff Allison previously worked for Aetna from December 1998 through May 2005. Then, in January 2009, he applied for another position at Aetna, whereby he input his personal information into Aetna's website. In May 2009, Plaintiff received a letter from Aetna stating that his personal information had been accessed by an unauthorized person.

9. Defendant Aetna, Inc. is a Pennsylvania corporation with its principal place of business located in Hartford, Connecticut. Aetna is a diversified healthcare benefits company that provides healthcare and related benefits, serving healthcare members, dental members, and group insurance customers. The Company offers medical, pharmacy, dental, behavorial health, group life and disability plans, and medical management capabilities and health care management services for Medicaid plans.

FACTUAL BACKGROUND

Security Breaches Lead to Identity Theft

10. By way of background, 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 committed or attempted, using a person's identifying information without authority. 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 governmental fraud. The Federal Trade Commission ("FTC") has stated that identity theft has been a serious problem in recent years, with approximately 9 million Americans as the victims of identity theft each year.[1]

11. 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.[2] As the GAO Report states, these data breaches involve the "unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers."

12. 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

---

[1] *See* "About Identity Theft," in FTC Publication, Fighting Back Against Identity Theft, *available at* http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

[2] *See* http://www.gao.gov/new.items/d07737.pdf

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.

13. In addition, the GAO states that victims of identity theft will face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

14. According to the Federal Trade Commission (FTC), nine million Americans have their identities stolen each year.[3] Identity theft victims must spend countless hours and money repairing damage to their good name and credit record. Identity thieves use stolen personal information such as social security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. In addition, a person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office, 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 has 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.[4]

15. 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

---

[3] *See* FTC Identity Theft Site, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

[4] http:///www.gao.gov/new.items/d07737.pdf (emphasis added).

official identification card in the victim's name but with their picture; using the victim's 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 personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

16. The unauthorized disclosure of a person's social security number can be particularly damaging since social security numbers cannot be easily replaced like a credit card. In order to obtain a new social security number, a person must show evidence that someone is using the number fraudulently or is being disadvantaged by the misuse.[5] Thus, a person whose personal information has been stolen cannot obtain a new social security number until the damage has already been done. Furthermore, obtaining a new social security number is not an absolute prevention against identity theft. Governmental agencies, private businesses, and credit reporting businesses likely still have the persons' records under the old number, and using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems. Since prior positive credit information is not associated with the new social security number, it is more difficult to obtain credit due to the absence of a credit history.

---

[5] Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327.

Aetna's Privacy Policy

17. Aetna represented to Plaintiff and the Class that it will protect their Sensitive Information. On Aetna's website, where it requested job applicants to provide their personal information, Aetna states: "All information will be held in the strictest confidence." The website also has a section entitled, "Web Privacy Statement." Under this section, Aetna states that:

> "Any nonpublic personal information that you may provide via our sites will be used solely for the purpose stated on the page where it is collected....Aetna will not sell, license, transmit or disclose this information outside of Aetna and its affiliated companies unless (a) expressly authorized by you, (b) necessary to enable Aetna contractors or agents to perform certain functions for us, or (c) required or permitted by law. In all cases, we will disclose the information consistent with applicable laws and regulations and we will require the recipient to protect the information and use it only for the purpose it was provided."

18. Also on its website, under a subheading entitled "Security," Aetna states as follows:

> "Aetna has adopted and adheres to stringent security standards designed to protect non-public personal information at aetna.com against accidental or unauthorized access or disclosure. Among the safeguards that Aetna has developed for this site are administrative, physical and technical barriers that together form a protective firewall around the information stored at this site. We periodically subject our site to simulated intrusion tests and have developed comprehensive disaster recovery plans."

19. Defendant failed to follow its own Privacy Policy and other representations noted above by maintaining an inadequate data security system which thereby allowed Sensitive Information of over 450,000 persons to be improperly accessed and misused by unauthorized persons.

The Data Breach At Aetna

20. Around May 27, 2009, Aetna publicly announced that its job application website was accessed by unauthorized persons.

21. As reported in the Associated Press that day, Aetna's website which was breached held email addresses for about 450,000 people who had applied for jobs or submitted resumes to the Company. Aetna stated that Social Security numbers of current and former employees and people who received job offers from the Company were stored on the website. For people who received job offers, the website also stored phone numbers, addresses, and employment histories.

22. Aetna's spokesperson Cynthia Michener is quoted as saying: "We know for certain that the emails were accessed, we don't know whether or not anything else was accessed." Michener said that some emails were copied from the website and then used to contract the job applicants.

23. Aetna has reportedly contacted 65,000 current and former employees whose Social Security numbers may have been compromised in the security breach. Aetna is offering such persons only one year of credit monitoring.

24. Aetna reportedly found out about the breach in early May 2009 when people complained to the Company that they had received spam messages that appeared to come from Aetna. The spam purported to be a response to a job inquiry and requested more personnel information from the affected persons.

25. No reason was given by Aetna for the delay of several weeks in notifying the public of the breach.

26. Significantly, Aetna had previously experienced another data breach in 2006,

when an employee's laptop was stolen. Over 38,000 persons were affected in that breach. Thus, Aetna was aware of the need for strict security protection over personal data, and the consequences that could result from a data breach.

27. Sometime in May 2009, Aetna sent a letter to certain persons affected by the recent security breach. In the letter, Aetna informed Plaintiff and the Class that there had been a security breach of Aetna's website, and that their Sensitive Information had been compromised. The letter also advised all affected persons to monitor their personal accounts for fraudulent charges, and to place a fraud alert on their credit files. The letter also stated that Aetna would provide affected persons with only one year of credit monitoring.

28. Thus, as a result of Aetna's unlawful conduct, Plaintiff's and Class members' Sensitive Information has been improperly accessed and misused by unauthorized persons.

29. Regarding Plaintiff Allison, he was employed at Aetna as an office assistant from December 1998 to May 2005. He worked in Aetna's office located in Blue Bell, Pennsylvania.

30. In January 2009, Plaintiff Allison went on to Aetna's website to apply for a customer service position. As required by Aetna, Plaintiff input his personal information and resume into Aetna's website.

31. In May 2009, Plaintiff Allison received a letter from Aetna, noted above, advising him of the data breach.

CLASS ACTION ALLEGATIONS

32. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this class action individually and on behalf of all other persons whose Sensitive Information was accessed from Aetna's job application website by unauthorized persons (the Class). The Class does not include Defendant, or its officers or directors.

33. On information and belief, the Class is compromised of hundreds of thousands of persons, making the joinder of such cases impracticable. Disposition of the claims in a class action will provide substantial benefits to both the parties and the Court.

34. The rights of each member of the Class were violated in a similar fashion based upon Defendant's uniform actions. Some common issues present here are:

a. Whether Defendant was negligent in collecting and storing Plaintiff's and Class members' Sensitive Information;

b. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class members' Sensitive Information;

c. Whether Defendant breached its duty to exercise reasonable care in storing Plaintiff's and Class members' Sensitive Information by storing that information on its computer systems in the manner in which it did;

d. Whether implied contracts existed between Defendant and Plaintiff and Class members;

e. Whether Plaintiff and the Class are at an increased risk of identity theft or other malfeasance as a result of Defendant's failure to protect the personal information of Plaintiff and the Class; and

f. Whether Plaintiff and Class members have sustained damages, and if so, what is the proper measure of those damages.

35. Plaintiff's claims are typical of the claims of the respective Class he seeks to represent, because the Sensitive Information of Plaintiff, like the Sensitive Information of all

members of the proposed Class, was improperly accessed and/or misused by unauthorized persons.

36. 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.

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

38. A class action is superior to all other available methods for the fair and efficient adjudication of Plaintiff's and Class members' claims. Plaintiff and Class members have suffered harm as a result of Defendant's conduct. Certification of a class action to resolve these disputes will reduce the possibility of repetitious litigation involving hundreds of thousands of class members. Further, certification is appropriate under Federal Rule of Civil Procedure 23, as the Class satisfies the requirements of Federal Rules of Civil Procedure 23 (a) and 23(b)(3).

COUNT I
NEGLIGENCE

39. Plaintiff repeats and realleges all preceding allegations as if fully set forth herein.

40. Defendant came into possession of Plaintiff's and Class members' Sensitive Information, and had a duty to exercise reasonable care in safeguarding and protecting such information from being compromised and/or stolen. This duty arose from, *inter alia*, the relationship between the parties, as well from Aetna's own Privacy Policy noted above.

41. Defendant had a duty to timely disclose that Plaintiff's and Class members' Sensitive Information within its possession had been, or was reasonably believed to have been, compromised. This duty arose from, *inter alia*, the relationship between the parties, as well from

state notification statutes.

42. Defendant had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class members' Sensitive Information. The breach of security, unauthorized access, and resulting harm to Plaintiff and the Class were reasonably foreseeable to Defendant, particularly in light of a prior data breach that occurred at Aetna in 2006.

43. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class members' Sensitive Information within Defendant's possession.

44. Defendant, through its actions and/or omissions, breached its duty to Plaintiff and Class members by failing to have procedures in place to detect and prevent access to Plaintiff's and Class members' Sensitive Information by unauthorized persons.

45. Defendant, through its actions and/or omissions, breached its duty to timely disclose the fact that Plaintiff's and Class members' Sensitive Information within its possession had been, or was reasonably believed to have been compromised.

46. But for Defendant's negligent and wrongful breach of its duties owed to Plaintiff and Class members, Plaintiff's and Class members' Sensitive Information would not have been compromised.

47. Plaintiff's and Class members' Sensitive Information was compromised and/or stolen as the proximate result of Defendant failing to exercise reasonable care in safeguarding such information by adopting, implementing, or maintaining appropriate security measures to protect and safeguard Plaintiff's and Class members' Sensitive Information within its possession.

48. Plaintiff and Class members suffered and will continue to suffer actual damages including, but not limited to, expenses and/or time spent on credit monitoring and identity theft insurance, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

COUNT II
BREACH OF IMPLIED CONTRACT

49. Plaintiff repeats and realleges all preceding allegations as if fully set forth herein.

50. Defendant came into possession of Plaintiff's and Class members' Sensitive Information and had implied contracts with Plaintiff and Class members to protect such information, by way of Plaintiff and Class members providing Defendant with the requisite employment information.

51. The implied contracts arose from the course of conduct between the Class and Aetna, the representations made by Aetna on its website concerning the safeguarding of employees' information, and the Privacy Policy set forth on Aetna's website. See ¶¶17-18 above.

52. The implied contracts required Defendant to not disclose Plaintiff's and Class members' Sensitive Information to unauthorized third party entities, and to safeguard and protect the information from being compromised and/or stolen.

53. Defendant did not safeguard and protect Plaintiff's and Class members' Sensitive Information from being compromised and/or stolen.

54. Because Defendant allowed unauthorized access to Plaintiff's and Class members' Sensitive Information and failed to safeguard and protect Plaintiff's and Class members' Sensitive Information from being compromised and/or stolen, Defendant breached its

contracts with Plaintiff and Class members.

55. Plaintiff and Class members suffered and will continue to suffer actual damages, including but not limited to the cost and time spent on credit monitoring and identify theft insurance, anxiety, emotional distress, loss of privacy, and other economic and noneconomic harm.

COUNT III
NEGLIGENT MISREPRESENTATION

56. Plaintiff realleges all preceding allegations as if fully set forth herein.

57. When requesting information from Plaintiff and the Class in connection with their job applications made over Aetna's website, Aetna made various affirmative representations on its website regarding its safeguarding of such information. Such representations are quoted at ¶¶17-18 of this complaint.

58. Aetna is liable for negligent misrepresentation in connection with these statements.

59. The above statements were material to Plaintiff and the Class in that they assured them that their Sensitive Information would be adequately protected.

60. Aetna made these misrepresentations while maintaining an inadequate security system, and thus Aetna should have known that its statements were false.

61. Aetna included the statements at issue in its Privacy Policy in order to induce Plaintiff and the Class to submit their Sensitive Information to Aetna.

62. In reliance on the misrepresentations, Plaintiff and the Class provided Aetna with their Sensitive Information which was compromised, thereby causing damage to Plaintiff and the Class.

63. Plaintiff and Class members suffered and will continue to suffer actual damages, including but not limited to the cost and time spent on credit monitoring and identify theft insurance, anxiety, emotional distress, loss of privacy, and other economic and noneconomic harm.

COUNT IV
INVASION OF PRIVACY

64. Plaintiff realleges all preceding allegations as if fully set forth herein.

65. Plaintiff and Class members have a legally-protected privacy interest in their Sensitive Information, and a reasonable expectation of privacy in such information. This right of privacy includes the right not to have someone else misappropriate and misuse such confidential personal information.

66. As a result of Defendant's unlawful actions, unauthorized intrusions were made into Plaintiff's and Class members' privacy when their Sensitive Information was accessed and/or misused without their knowledge, authorization, or consent. This unauthorized access and/or misuse of such private information is one that is highly offensive or objectionable to a reasonable person. Moreover, the disclosure of such private information, as alleged herein, does not include information that is of a legitimate public concern.

67. Defendant violated the rights of privacy of Plaintiff and Class members by allowing the access and/or misuse of their Sensitive Information without their consent.

68. As a result of the unlawful conduct, as alleged herein, the privacy rights of Plaintiff and Class members have been violated, and Plaintiff and Class members have been harmed as a result.

69. Plaintiff and Class members suffered and will continue to suffer actual damages, including but not limited to the cost and time spent on credit monitoring and identify theft insurance, anxiety, emotional distress, loss of privacy, and other economic and noneconomic harm.

JURY TRIAL DEMANDED

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

PRAYER FOR RELIEF

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

a. For an order certifying the proposed nationwide Class herein under Federal Rule of Civil Procedure 23(a) and (b)(3) and appointing Plaintiff and Plaintiff's counsel to represent said Class;

b. Finding that Defendant is liable under all of the legal claims asserted herein for its failure to safeguard and protect Plaintiff's and Class members' Sensitive Information stored on its computer systems and in its physical possession;

c. Enjoining Defendant from actions which places employees and the Class at a risk of future security breaches;

e. Requiring Defendant to identify to Plaintiff the persons who improperly accessed the Sensitive Information;

f. Award injunctive relief, including but not limited to: (i) the provision of credit monitoring and/or credit card monitoring services for the Class; (ii) the provision of identity theft insurance for the Class; and (iii) the requirement that Defendant receive periodic compliance audits by a third party regarding the security of its computer systems used for processing and storing personal employee or customer data;

h. Award compensation to Plaintiff and the Class as a result of the unauthorized access to their Sensitive Information;

i. Awarding damages to Plaintiff and Class members under the common law theories alleged herein;

j. Awarding statutory, punitive, and/or treble damages as provided under relevant laws;

k. Entering declaratory relief as this Court deems appropriate;

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

m. For an order awarding pre-judgement and post-judgement interest as prescribed by law; and

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

Respectfully submitted,

Dated: June 5, 2009

BERGER & MONTAGUE, P.C.

By SRS187 (Validation Code)

Sherrie R. Savett, Esq. (Pa. I.D. No.17646)
Michael T. Fantini, Esq. (Pa. I.D. No. 57192)
Jon Lambiras, Esq. (Pa. I.D. No.92384)
1622 Locust Street
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4636

SHELLER, P.C.
Jamie L. Sheller, Esq. (Pa. I.D. No. 55722)
1528 Walnut Street, 3rd Floor
Philadelphia, PA 19102
Tel: (215) 790-7300
Fax: (215) 546-0942

Counsel for Plaintiff and the Class

malta467938-002.doc