UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
Case No. 10-cv-24513-JLK

JUANA CURRY and WILLIAM MOORE, individually and on behalf of a class of similarly situated individuals, Plaintiffs, v. AVMED, INC., d/b/a AvMed, a Florida Corporation Defendant.	The Honorable James Lawrence King

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiffs Juana Curry ("Curry") and William Moore ("Moore") (collectively referred to as "Plaintiffs") bring this Second Amended Class Action Complaint against AvMed Inc., ("AvMed" or "Defendant"), and allege as follows, upon personal knowledge as to themselves and their own acts and experiences, and as to all other matters, upon information and belief, including investigation conducted by their attorneys.

NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of Plaintiffs and all other persons similarly situated against AvMed for its failure to adequately protect the confidential personal and medical information of its current and former customers—conduct that ultimately resulted in the largest medical data breach in history.

2. On or about December 10, 2009, two unencrypted laptop computers were stolen from AvMed's Gainesville, Florida corporate office (the "data breach"). The laptops contained private, personal information including, but not limited to, protected health information as

defined by the Health Insurance Portability and Accountability Act ("HIPAA"), Social Security numbers ("SSNs"), medical information and other information (collectively, "Sensitive Information") of approximately 1.2 million AvMed enrollees.

3. As a result of AvMed's failure to implement and follow basic security procedures, Plaintiffs' Sensitive Information is now in the hands of thieves. Plaintiffs now face a substantial increased risk of identity theft; in fact, Curry and Moore have already experienced repeated instances of identity theft since the data breach. Indeed, numerous individuals whose Sensitive Information was compromised due to AvMed's failure to protect their confidential data have already fallen victim to identity theft. Consequently, AvMed's current and former customers have had to spend, and will continue to spend, significant time and money in the future to protect themselves.

4. Additionally, as a result of AvMed's failure to follow contractually-agreed upon, federally-prescribed, industry standard security procedures, Plaintiffs received only a diminished value of the services they paid AvMed to provide. Plaintiffs contracted for an insurance plan that included a guarantee by AvMed to safeguard their personal information, and instead, received a plan devoid of these very important protections. Accordingly, Plaintiffs allege claims for breach of contract, breach of implied contract, breach of implied covenant of good faith and fair dealing, unjust enrichment, violation of Fla. Stat. § 395.3025, negligence, negligence per se, and breach of fiduciary duty.

JURISDICTION AND VENUE

5. The Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because (a) at least one member of the putative class is a citizen of a state different from Defendant, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs,

and (c) none of the exceptions under the subsection apply to this action.

6. Venue is proper pursuant to 28 U.S.C. § 1391(a)(1)-(2) because AvMed is a corporation headquartered in this judicial district and a substantial part of the events giving rise to Plaintiffs' claims occurred in this judicial district.

PARTIES

7. Plaintiff Curry is a current resident of Florida. As an AvMed member, Curry provided Sensitive Information to Defendant. Curry's Sensitive Information was contained on an unprotected and unencrypted laptop computer that was stolen in the data breach. As a result of the data breach, Curry's identity was stolen.

8. Plaintiff Moore is a current resident of Florida. As an AvMed member, Moore provided Sensitive Information to Defendant. Moore's Sensitive Information was contained on an unprotected and unencrypted laptop computer that was stolen in the data breach. As a result of the data breach, Moore's identity was stolen.

9. Defendant AvMed is a Florida corporation headquartered in Miami, Florida. AvMed is an integrated managed care organization that delivers managed health care services through health plans and government sponsored managed care plans to more than 1.2 million individuals throughout the State of Florida and the United States.

FACTUAL BACKGROUND

Security Breaches Lead to Identity Theft

10. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as SSNs to open financial accounts, receive government benefits and incur charges and credit in a person's

name.[1] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records...[and their] good name."

11. According to the Federal Trade Commission ("FTC"), identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[2] Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[3]

12. With access to an individual's Sensitive Information, criminals are capable of conducting many nefarious actions besides emptying the victim's bank account. 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 the thief's picture; using the victim's name and SSN 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 SSN, rent a house or receive medical services in the victim's name, and may even give the victim's personal

---

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

[2] *See* FTC Identity Theft Website: www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html.

[3] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id.*

information to police during an arrest resulting in an arrest warrant being issued in the victim's name.[4] Further, loss of private and personal health information can expose the victim to loss of reputation, loss of job employment, black mail and other negative effects.[5]

13. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [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.

14. Sensitive Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[6] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Sensitive Information directly on various Internet websites making the information publicly

---

[4] *See* FTC Identity Theft Website, *supra*.

[5] *See* http://www.pueblo.gsa.gov/cic_text/money/preventidtheft/preventing.pdf (stating that identity thieves "may threaten national security or commit acts of terrorism" and noting that the September 11 hijackers used fake ID's to board their planes); *see also* www.msnbc.msn.com/id/5594385 (stating that the September 11 hijackers "liberally used document fraud prior to that date, some to ease entrance into the United States, others to move around once they were here and to obtain drivers' licenses they needed to board the airplanes.")

[6] Companies, in fact, also recognize Sensitive Information as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market. Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html. *See also* T. Soma, ET AL, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009).

available. In one study, researchers found hundreds of websites displaying stolen Sensitive Information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism—the "Safe Browsing list." The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[7]

15. A similar recent report about health-care related identity theft fraud sponsored by Experian indicated that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000."[8] Moreover, a majority of the victims were forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage. Almost 50 percent of the victims lost their health care coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Forty (40) percent of the consumers were never able to resolve their identity theft at all. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.[9]

16. The FTC recently indicated that South Florida has the highest rate of identify theft complaints in the entire United States.[10]

AvMed's Privacy Policy and Agreements to Keep Sensitive Information Confidential

---

[7] http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/

[8] http://news.cnet.com/8301-27080_3-10460902-245.html

[9] *See, e.g.*, Soma, *supra*, at *3-4.

[10] http://blogs.sun-sentinel.com/consumerblog/2011/04/05/florida-ranks-number-2-for-fraud-id-theft-by-ftc-south-florida-worst-place-in-state/

17. AvMed represented to Plaintiffs and the Classes that it would protect their Sensitive Information.

18. Through its website, AvMed states the following confidentiality and privacy policy:

> **Your Privacy**
>
> We follow the Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations to safeguard your protected health information (PHI). *We do not disclose information about you or any former members to anyone, except as permitted by HIPAA.* All AvMed employees sign a confidentiality statement and are trained in the proper handling of personal information. Each time you call Member Services, you will be asked to verify your AvMed member ID number, address, phone number and date of birth. If you're calling for another AvMed member, you need to identify yourself, relationship to the member you're calling about, and verify the member's ID number, address, phone number and date of birth.

(*See* "Protecting Your Privacy," a true and accurate copy of which is attached hereto as Exhibit A.)

19. On its website, Defendant also enumerates the rights and responsibilities required of AvMed and its members:

> **Members' Rights and Responsibilities**
>
> ***Members have a right to:***
>
> ***** ***** *****
>
> The confidentiality of information about their medical health condition being maintained by the Plan and the right to approve or refuse the release of member specific information including medical records, by AvMed, except when the release is required by law.
>
> * * *
>
> ***Members have the responsibility to:***
>
> ***** ***** *****

> Provide accurate and complete information about their health.
>
> * * *
>
> Fulfill financial obligations for receiving care, as required by their health plan agreement, in a timely manner.

(*See* "Members' Rights and Responsibilities," a true and accurate copy of which is attached hereto as Exhibit B.)

20. Additionally, in recognizing the confidential and sensitive nature of the information it collects from members, AvMed adopted, and advertises on its website, a confidentiality policy with respect to Sensitive Information:

> Confidentiality
>
> AvMed and its employees are in possession of and have access to a wealth of confidential, sensitive and proprietary information. The inappropriate release of such information could be detrimental to AvMed, as well as its members, clients, providers, and/or vendors. Every AvMed employee has an obligation to actively protect and safeguard confidential, sensitive and proprietary information in a manner designed to prevent its unauthorized disclosure.
>
> 1) AvMed employees have an obligation to maintain the confidentiality of member information in accordance with all applicable laws and regulations, including, but not limited to, the HIPAA Privacy and Security standards. Employees are reminded that information requiring protection exists in many formats, such as paper, electronic, audio, and video. All copies, formats and versions of member information must be maintained in accordance with applicable laws and AvMed policies and procedures. AvMed assigns employee access to confidential information through a role based security approach to ensure that only those staff whose jobs require it and who have a legitimate need-to-know, have the ability to access confidential member data. Employees must not share passwords or other system access rights with any other employee or person(s). Employees are instructed to always make sure that any access or use of confidential data is carried out using only the minimum amount necessary. Additionally, employees shall refrain from revealing any personal or confidential information unless supported by legitimate business or member care purposes. If the disclosure of information is so supported, employees shall use or disclose on a need-to-know basis, only the

> minimum amount necessary to accomplish the task. If questions arise regarding an obligation to maintain the confidentiality of information or the appropriate release of information, employees should seek assistance from a supervisor, the Compliance department or other appropriate staff within the AvMed Legal Department.
>
> 2) Information, ideas and intellectual property assets of AvMed are important to its success. Information pertaining to competitive position, business strategy, payment and reimbursement information, and information relating to negotiations with third parties or other employees should be protected and shared only with those individuals having a need to know such information in order to perform their job responsibilities.
>
> 3) Salary, benefit and other personal information relating to employees shall be treated as confidential. Personnel files, payroll information, disciplinary matters and similar information shall be maintained in a manner designed to ensure confidentiality in accordance with applicable laws.
>
> 4) Employees will exercise due care to prevent the unauthorized release or sharing of information. To ensure that employees fully understand the importance of upholding this particular standard of conduct, they are required to sign a Statement of Confidentiality at the time of hire and on an annual basis thereafter.

(*See* "Code of Ethical Business Conduct," a true and accurate copy of which is attached hereto as Exhibit C.)

21. AvMed requires its members to enter into a Service Contract to disclose Sensitive Information, which compels members to "provide accurate and complete information about their health." In exchange, AvMed promises that:

> **Your medical and claims records are confidential**
>
> We will keep your medical and claims records confidential. Please note that we may disclose your medical and claims information (including your prescription drug utilization) to any of your treating physicians or dispensing pharmacies.

(*See* "Health Plans," a true and accurate copy of which is attached hereto as Exhibit D.)

22. These representations and requirements are collectively provided on AvMed's webpage that lists member responsibilities and member rights under their plans. AvMed created these representations and requirements and publicly advertised them on its website as a means of increasing the value of its insurance policies, thus allowing it to charge consumers higher premiums. This agreement is the same for all AvMed members, including Plaintiffs and the Classes.

The Data Breach at AvMed

23. On or about December 10, 2009, two laptop computers that were owned, operated, and controlled by AvMed were stolen from AvMed's corporate office in Gainesville, Florida. The two laptop computers contained the Sensitive Information of AvMed members, including Plaintiffs and the Classes. The stolen data encompassed Sensitive Information dating back to April 2003.

24. On or about December 23, 2009, AvMed officials determined that at least one of the stolen laptop computers was not encrypted to protect access to, and widespread dissemination of, AvMed's members' Sensitive Information.

25. Upon information and belief, the thief sold the unencrypted, unprotected AvMed laptop computer to an individual who has a history of dealing in stolen property.

26. In addition to failing to secure its members' Sensitive Information, AvMed failed to adequately investigate the breach to determine how many of its members' Sensitive Information had been exposed, or in the alternative, willfully failed to disclose the scope and expanse of the breach.

27. On or about February 3, 2010, AvMed, for the first time, publicly revealed the security breach and notified the 360,000 potentially affected members.

28. On or around February 5, 2010, AvMed sent a letter to Plaintiffs and other Class members notifying them of the data breach ("February Letter"). (*See* February Letter, a true and accurate copy of which is attached hereto as Exhibit E.) The February Letter was prepared and drafted by AvMed. In deliberate disregard to the fact that the stolen laptop computer was unencrypted, unprotected, and readily viewable by unauthorized third parties, AvMed downplayed the seriousness of the incident by informing Plaintiffs and the Classes that the Sensitive Information "was listed in such a way that the risk of identity theft is very low[.]" (Ex. E).

29. AvMed then hired a forensics team from PriceWaterhouseCoopers ("PWC") to provide an independent analysis of the number of potentially affected members. Significantly, PWC was not hired by AvMed until *after* its February 3, 2010 public disclosure of the data breach.

30. AvMed took no action to promptly notify its members that were affected by the data breach.

31. AvMed waited until June 3, 2010—one hundred and seventy-four (174) days after the initial breach was discovered—to finally disclose that an *additional 860,000* current and former members were affected by the data breach and that their unencrypted and unprotected Sensitive Information was contained on a stolen laptop that was sold to, on information and belief, an individual who has a history of dealing in stolen property.

32. On or around June 7, 2010, AvMed sent a letter to Plaintiffs and other Class members notifying them that the data breach was three times as large as originally disclosed by AvMed ("June Letter"). (*See* June Letter, a true and accurate copy of which is attached hereto as Exhibit F.) The June Letter was prepared and drafted by AvMed.

33. AvMed's failure to notify its members of this data breach until six months after it occurred meant that those members, including Plaintiffs and the other members of the Classes, had no reason to check their accounts and credit reports for suspicious activity arising from the breach during that time.

34. AvMed, knowing that Sensitive Information is subject to the strict privacy and security protections of HIPAA, and other standards and regulations, delayed and otherwise failed to properly and timely provide notice to Plaintiffs and the other members of the Classes regarding the stolen Sensitive Information.

35. AvMed designed and implemented its policies and procedures regarding the security of protected health information and Sensitive Information. These policies and procedures failed to adhere to reasonable and best industry practices in safeguarding protected health information and other Sensitive Information. For instance, AvMed failed to encrypt the stolen laptop computers or otherwise safeguard the Plaintiffs' and Class members' Sensitive Information.

36. Further, AvMed did not notify Plaintiffs or Class Members whose Sensitive Information was, or was reasonably believed to have been, accessed by an unauthorized person through the data breach in any manner, including but not limited to, written, telephone, electronic or authorized substitute notice until AvMed posted a notice on its website on or about June 3, 2010 and began sending letters in a rolling mailing on or about June 7, 2010.

37. Upon information and belief, AvMed failed to effectively supervise its workforce (including both employees and independent contractors) on the policies and procedures with respect to the appropriate maintenance, use and disclosure of protected health information and other Sensitive Information.

38. In a June 7, 2010 update to AvMed's "Frequently Asked Questions" regarding the breach, AvMed admitted that "During the recovery process and internal investigation, **AvMed determined that the data on the laptops was not properly secure**." (*See* "Frequently Asked Questions," a true and accurate copy of which is attached hereto as Exhibit G.)

39. Minors were among the AvMed members whose Sensitive Information was exposed on the unencrypted and unprotected laptop.

40. In sum, AvMed's failure to encrypt and otherwise safeguard their laptop computers resulted in the exposure of the Sensitive Information of approximately 1.2 million current and former AvMed members.

41. As members of AvMed, Plaintiffs Curry and Moore provided AvMed with their accurate Sensitive Information, as required under their Service Contracts. The stolen laptop computers contained their unencrypted, unprotected Sensitive Information.

42. Plaintiffs' Sensitive Information was thereafter sold to, upon information and belief, an individual who has a history of dealing in stolen property, thus substantially increasing the likelihood that their identity would be stolen.

Curry's Identity Was Stolen and She Suffers From Monetary Injuries

43. Curry has suffered from identity theft as a direct result of AvMed's failure to safeguard and protect her Sensitive Information.

44. Curry's identity was stolen and, in or around October 2010, it was used to open bank accounts with Bank of America and activate credit cards in her name.

45. The credit cards were then used to make several unauthorized purchases, causing Curry to incur fraudulent credit card charges.

46. Curry's Sensitive Information was also used to change her home address with the U.S. Postal Service.

47. As a direct result of AvMed's data breach, Curry was forced to spend money placing alerts with various credit reporting companies and contesting the fraudulent charges made in her name.

48. As a direct result of AvMed's data breach, Curry was also forced, and continues, to spend $17.00 per month for a subscription to LifeLock, an identity theft protection service. Curry will continue to have this expenditure as a result of AvMed's data breach.

49. As a direct result of AvMed's data breach, Curry was also forced to miss work and incur significant lost wages in order to spend time meeting with the police to report and attempt to remedy the effects of the AvMed data breach.

50. Before October 2010, Curry had never been the victim of identity theft.

51. As a direct result of AvMed's data breach, Curry has spent money on a variety of out-of-pocket costs—including, but not limited to, travel-related costs, cellular telephone minutes, postage, and credit monitoring services—to get fraudulent charges removed from her credit. Additionally, she has lost wages and goodwill at her place of employment because of time she has had to miss in attempting to remedy the effects of AvMed's data breach.

The Data Breach Caused Curry's Identity Theft and Monetary Injuries

52. AvMed's data breach caused Curry's identity theft.

53. *Prior to the data breach, Curry's identity had never been stolen.*

54. Furthermore, prior to the data breach, Curry's Sensitive Information had never been compromised in any way.

55. Indeed, Curry took substantial precautions to protect herself from identity theft. Curry has *never* transmitted her Sensitive Information over the Internet, or any other unsecured source, and has never even stored her Sensitive Information on a computer or media device. Curry stores documents containing Sensitive Information in a safe and secure physical location and destroys any documents she receives in the mail that contain any of her Sensitive Information, or that contain any information that could otherwise be used to steal her identity, such as credit card offers.

56. However, as explained above, Curry has experienced—for the first time in her life—numerous instances of identity theft, which was caused by AvMed's data breach.

57. Thus, given that before the data breach, Curry had never previously suffered from identity theft and undertook substantial efforts to protect her identity, Curry has sufficiently shown that the data breach caused his identity theft.

58. In short, but for AvMed's data breach, Curry's identity would not have been stolen.

Moore's Identity Was Stolen and He Suffers From Monetary Injuries

59. Like Curry, Moore has suffered from identity theft as a direct result of AvMed's failure to safeguard and protect his Sensitive Information.

60. Moore's identity was stolen and, in or around February 2011, used to open a bank account with E*Trade Financial in his name.

61. The E*Trade Financial bank account was opened by an individual using Moore's Sensitive Information.

62. On April 5, 2011, The E*Trade Financial bank account opened in Moore's name was overdrawn by $4,298.77 by an unauthorized third party. (*See* "E*Trade Letter," a true and accurate copy of which is attached hereto as Exhibit H.)

63. Despite the fact that Moore has reported the identity theft to E*Trade Financial, E*Trade Financial holds Moore responsible for the overdrawn amount of $4,298.77. (Ex. H.)

64. Accordingly, Moore suffers real and actual monetary damages in the amount of $4,298.77.

65. Before February 2011, Moore had never been the victim of identity theft.

66. As a direct result of AvMed's data breach, Moore has spent money on a variety of out-of-pocket costs including, but not limited to, travel-related costs, cellular telephone minutes, postage, and credit monitoring services.

The Data Breach Caused Moore's Identity Theft and Monetary Injuries

67. AvMed's data breach caused Moore's identity theft.

68. *Prior to the data breach, Moore's identity had never been stolen.*

69. Furthermore, prior to the data breach, Moore's Sensitive Information had never been compromised in any way.

70. In fact, beginning several years prior to the data breach and continuing to this day, Moore regularly monitors his credit for unusual activity.

71. Indeed, Moore took substantial precautions to protect himself from identity theft. Moore has *never* transmitted unencrypted Sensitive Information over the internet, or any other unsecured source. Moore stores documents containing Sensitive Information in a safe and secure physical location and destroys any documents he receives in the mail that contain any of his

Sensitive Information, or that contain any information that could otherwise be used to steal his identity.

72. However, as explained above, Moore has experienced—for the first time in his life—identity theft, which was caused by AvMed's data breach.

73. Thus, given that before the data breach, Moore had never previously suffered from identity theft and undertook substantial efforts to protect his identity, Moore has sufficiently shown that the data breach caused his identity theft.

74. In short, but for the data breach, Moore's identity would not have been stolen.

AvMed's Credit Monitoring Offer is Inadequate

75. AvMed offered the Plaintiffs and Class members two years of Debix Credit monitoring services.

76. AvMed's mere two-year offer of Debix is a woefully insufficient remedy for Defendant's data breach. As discussed, victims of data breaches commonly face multiple years of ongoing identity theft.

77. The Debix monitoring program does not provide any compensation for the release of Plaintiffs' and Class members' Sensitive Information, including medical information.

78. In addition, AvMed's credit monitoring offer to Plaintiffs and the Classes squarely placed the burden on them, rather than AvMed, to investigate and protect themselves from AvMed's tortious acts resulting in the data breach. Rather than automatically enrolling Plaintiffs and the Classes in Debix's credit monitoring program upon discovery of the breach, AvMed instead sent instructions to affected members recommending that they sign-up for these services. Upon information and belief, this was done in an attempt by AvMed to mitigate the costs associated with its data breach. AvMed knows, or should have known, that many of its

members, many of whom are infirm, are not technically-savvy and would not fully grasp the magnitude and significance of its data breach, and thus would fail to sign up for Debix's services.

79. Furthermore, AvMed instructed its enrollees, including Plaintiffs and Class members, to notify the three credit bureaus to discuss placing a fraud alert on their credit reports, regularly review all medical bills and benefits statements, order and check all credit reports—all at their own time and expense. (Ex. F, pp. 2-3.)

80. Likewise, AvMed failed to acquire any identity theft insurance coverage or enrollment in fraud resolution services for Plaintiffs and the Class members.

AvMed's Wrongful Conduct in Violation of HIPAA and Industry-Standard Practice

81. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Sensitive Information like the data left unguarded by AvMed. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

82. AvMed's data breach resulted from a combination of insufficiencies that indicate Defendant did not comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from AvMed's data breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures prohibiting storing Sensitive Information on portable computers (such as a laptops) and/or information security policies or procedures in place regarding encrypting or protecting Sensitive Information.

83. In addition, AvMed's data breach could have been prevented if AvMed implemented HIPAA mandated, industry standard policies and procedures for securely disposing of Sensitive Information when it was no longer necessary and/or had honored its obligations to its members.

84. Contributing to the problem was AvMed's failure to effectively supervise and train its employees that were in charge of designing and implementing policies and procedures on the appropriate maintenance, use, and disclosure of Sensitive Information.

85. AvMed's security failures also include, but are not limited to, the following:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to adequately catalog the location of members' digital information;

d. Failing to encrypt Sensitive Information of Plaintiffs and Class Members;

e. Failing to ensure the confidentiality and integrity of electronic protected health information it created, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

g. Failing to implement technical policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility to maintain their security in violation of 45 CFR 164.310(d)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

i. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

j. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

k. Failing to protect against an reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

l. Failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(94);

m. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502 et seq.;

n. Failing to effectively train all members of its workforce (including independent contractors involved in the data breach) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions

and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45CFR 164.308(a)(5); and

o. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR164.530(c).

86. AvMed also failed to comply with industry standards. In November 2001, the National Institute of Standards and Technology ("NIST") proposed an "Advanced Encryption Standard" ("AES") to be used as the technological standard for encrypting sensitive data.[11] On May 26, 2002, AES was adopted as the standard encryption technique of the United States government. AES is free for any use private or public, commercial or non-commercial.

87. The NIST published a report in March 2005 detailing standards for healthcare providers to comply with HIPAA's Security Rule. In the Report, the NIST recommends specific techniques to safeguard electronically stored Sensitive Information. In one example, the NIST specifically recommends a system, easily implemented and maintained, to automatically encrypt Sensitive Information during non-work hours, and then decrypt it at the beginning of each workday.[12]

---

[11] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEP'T OF COMMERCE, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION PUBL'N 197 "Announcing the Advanced Encryption Standard" (2001), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[12] MATTHEW SCHOLL ET AL., NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEP'T OF COMMERCE. NIST SPECIAL PUBLICATION 800-66 REVISION 1, AN INTRODUCTORY RESOURCE GUIDE FOR IMPLEMENTING THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

88. In light of the foregoing, AvMed has failed to comply with industry standards. Even more striking is that one of the exact examples recommended by the NIST, encrypting data during non-work hours—a free and commonly used technique—if implemented, would have prevented the data breach and the identity theft of its members.

CLASS ALLEGATIONS

89. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of themselves and a Class and two Subclasses defined as follows:

The Class: Plaintiffs Juana Curry and William Moore bring this action on behalf of themselves and a Class of similarly situated individuals, defined as follows:

> All individuals in the United States that are current or former members of healthcare plans provided by AvMed, Inc. and whose Sensitive Information was stored on the unencrypted AvMed laptops stolen on December 11, 2009.

The Identity Theft Subclass: Plaintiffs Juana Curry and William Moore bring this action on behalf of herself and a Subclass of similarly situated individuals, defined as follows:

> All individuals in the United States that are current or former members of healthcare plans provided by AvMed, Inc., whose Sensitive Information was stored on the unencrypted AvMed laptop stolen on December 11, 2009, and who have experienced identity theft as a result of AvMed's data breach.

Excluded from the Classes are (i) any judge presiding over this action and members of their families; (ii) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest and their current or former employees, officers and directors; (iii) persons who properly execute and file a timely request for exclusion from the Classes; and (iv) the legal representatives, successors or assigns of any such excluded persons, as well as any individual who contributed to the unauthorized access of

---

SECURITY RULE, at 41 (2008), http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-

AvMed's laptops.

90. **Numerosity:** The exact number of members of the Classes is unknown to Plaintiffs at this time, but on information and belief, there are at least 1.2 million members of the Classes throughout the country, making joinder of each individual member impracticable. Ultimately, the members of the Classes will be easily identified through Defendant's records.

91. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of the Classes. Plaintiffs and the Classes sustained damages as a result of Defendant's uniform wrongful conduct during transactions with Plaintiffs and the Classes.

92. **Adequate Representation:** Plaintiffs will fairly and adequately represent and protect the interests of the Classes, and have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Classes, and Defendant has no defenses unique to Plaintiffs.

93. **Predominance and Superiority:** This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Classes is impracticable. The damages suffered by the individual members of the Classes will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual members of the Classes to obtain effective relief from Defendant's misconduct. Even if members of the Classes could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class

---

66-Revision1.pdf.

action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

94. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Classes, and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply and affect members of the Classes uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

95. **Commonality:** Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting only individual members, and include, but are not limited to:

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

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

c. Whether Defendant breached its duty to exercise reasonable care in handling Plaintiffs' and Class members' Sensitive Information by storing that information on its laptop computers in the manner alleged herein;

d. Whether Defendant notified Plaintiffs and the Classes of the data breach within a reasonable amount of time;

e. Whether implied or express contracts existed between Defendant, on the one hand, and Plaintiffs and the Class members on the other;

f. Whether storing Sensitive Information in an unencrypted format was reasonable under industry standards;

Plaintiffs reserve the right to revise Class definitions based on facts learned in discovery.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Classes)

96. Plaintiffs repeat and re-allege all previous allegations as if fully set forth herein.

97. Defendant requested and came into possession of Plaintiffs' and members of the Classes' Sensitive Information, and had a duty to exercise reasonable care in safeguarding and protecting such information from being accessed. Defendant's duty arose from the industry standards discussed above and its relationship with Plaintiffs.

98. Defendant had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and members of the Classes' Sensitive Information. The breach of security, unauthorized access, and resulting injury to Plaintiffs' and the Classes were reasonably foreseeable, particularly in light of Defendant's inadequate data security system and failure to encrypt the data.

99. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Classes by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiffs' and Class members' Sensitive Information within Defendant's control.

100. Defendant, through its actions and/or omissions, breached its duty to Plaintiffs and the Class members by failing to have procedures in place to detect and prevent access to

Plaintiffs' and members of the Classes' Sensitive Information by unauthorized persons.

101. But for Defendant's breach of its duties, Plaintiffs' and members of the Classes' Sensitive Information would not have been compromised.

102. Plaintiffs' and members of the Classes' Sensitive Information was stolen and accessed as the proximate result of Defendant failing to exercise reasonable care in safeguarding such information by adopting, implementing, and maintaining appropriate security measures and encryption.

103. As a result of Defendant's conduct, Plaintiffs and members of the Classes have suffered actual identity theft. Plaintiffs 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; time spent scrutinizing bank statements, credit card statements, and credit reports; missed wages; expenses and/or time spent initiating fraud alerts; and, the diminished value of the AvMed services they received. Plaintiff Moore has also suffered actual damages in the amount of $4,298.77. Plaintiffs and members of the Classes have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT II
Breach Of Contract
(On Behalf of Plaintiffs and the Classes)

104. Plaintiffs repeat and re-allege all previous allegations as if fully set forth herein.

105. Plaintiffs paid money to AvMed in exchange for health care coverage and its promises to protect their health information and Sensitive Information.

106. In its written services contract, AvMed expressly promised Plaintiffs and members of the Classes that AvMed only discloses health information when required to do so by

federal or state law. AvMed further promised that it would protect their Sensitive Information.

107. AvMed promised to comply with all HIPAA standards and to make sure that Plaintiffs' and members of the Classes' health information was protected. AvMed further promised to provide notice to Plaintiffs and members of the Classes describing AvMed's legal duties and privacy practices with respect to their health information.

108. The contracts required Defendant not to disclose Plaintiffs' and members of the Classes' health information and Sensitive Information to unauthorized third parties, and to safeguard the information from being lost and accessed. (Ex. B).

109. Defendant did not safeguard Plaintiffs' and members of the Classes' protected health information and Sensitive Information. Further, AvMed did not comply with its promise to abide by HIPAA.

110. The failure to meet these promises and obligations constitute an express breach of contract.

111. Because Defendant allowed unauthorized access to Plaintiffs' and members of the Classes' Sensitive Information and failed to safeguard the Sensitive Information, Defendant breached its contracts with Plaintiffs and members of the Classes.

112. A meeting of the minds occurred, as Plaintiffs and members of the Classes agreed, *inter alia,* "to provide accurate and complete [Sensitive Information]" and to pay AvMed in exchange for AvMed's agreement to, among other things, protect their Sensitive Information. (Ex. B.)

113. AvMed breached the contract by not meeting the minimum level of protection of Plaintiffs' and members of the Classes' health information, because it did not prevent against the breach of 1.2 million members' Sensitive Information.

114. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in AvMed providing services to Plaintiffs and the Classes that were of a diminished value.

115. As a result of Defendant's conduct, Plaintiffs and members of the Classes have suffered actual identity theft. Plaintiffs 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; time spent scrutinizing bank statements, credit card statements, and credit reports; missed wages; expenses and/or time spent initiating fraud alerts; and, the diminished value of the AvMed services they received. Plaintiff Moore has also suffered actual damages in the amount of $4,298.77. Plaintiffs and members of the Classes have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT III
Breach of Implied Contracts (in the alternative to Breach of Contract)
(On Behalf of Plaintiffs and the Classes)

116. Plaintiffs repeat and re-allege paragraphs 1-88 as if fully set forth herein.

117. Plaintiffs hereby plead this count in the alternative to their breach of contract claim.

118. In order to benefit from Defendant's healthcare plan, Plaintiffs and the Classes disclosed Sensitive Information to AvMed, including their names, contact information (addresses, phone and fax numbers and email addresses), Social Security Numbers, dates of birth, and extremely sensitive medical diagnosis information.

119. By providing that Sensitive Information and upon Defendant's acceptance of such information, Plaintiffs and the Classes, on the one hand, and Defendant, on the other hand,

entered into implied contracts whereby Defendant was obligated to take reasonable steps to secure and safeguard that information.

120. Under the implied contract, Defendant was further obligated to provide Plaintiffs and the Classes with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information.

121. Without such implied contracts, Plaintiffs and the Classes would not have provided their personal information to Defendant.

122. Defendant breached its duty to Plaintiffs and the Classes by:

a. Failing to encrypt or otherwise protect the laptops containing Plaintiffs' and the Class members' and the Subclass members' Sensitive Information;

b. Failing to timely notify and/or warn Plaintiffs and the Class members and the Subclass members of the data breach;

c. Failing to ensure the confidentiality and integrity of electronic protected health information it created, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement technical policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility to maintain their security in violation of 45 CFR 164.310(d)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against an reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(94);

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502 et seq.;

l. Failing to effectively train all members of its workforce (including independent contractors involved in the data breach) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45

CFR 164.530(b) and 45CFR 164.308(a)(5);

m. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR164.530(c); and

n. Otherwise failing to safeguard Plaintiffs' and the Class members and the Subclass members' Sensitive Information.

123. As a result of Defendant's conduct, Plaintiffs and members of the Classes have suffered actual identity theft. Plaintiffs 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; time spent scrutinizing bank statements, credit card statements, and credit reports; missed wages; expenses and/or time spent initiating fraud alerts; and, the diminished value of the AvMed services they received. Plaintiff Moore has also suffered actual damages in the amount of $4,298.77. Plaintiffs and members of the Classes have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT IV
Restitution/Unjust Enrichment (in the alternative to Breach of Contract)
(On Behalf of Plaintiffs and the Classes)

124. Plaintiffs repeat and re-allege Paragraphs 1-103 as if fully set forth herein.

125. Plaintiffs hereby plead Count IV in the alternative to Count II.

126. Plaintiffs and members of the Classes conferred a monetary benefit on Defendant. Defendant received and retained money belonging to Plaintiffs and the Classes in the form of monthly premiums they pay to AvMed.

127. Defendant appreciates or has knowledge of such benefit.

128. The monthly premiums that Plaintiffs and the Classes pay to AvMed used by AvMed, in part, to pay for the administrative costs of data management and security.

129. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and members of the Classes, because Defendant failed to implement the data management and security measures that are mandated by industry standards.

130. As a result of Defendant's conduct, Plaintiffs and members of the Classes have suffered actual identity theft. Plaintiffs 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; time spent scrutinizing bank statements, credit card statements, and credit reports; missed wages; expenses and/or time spent initiating fraud alerts; and, the diminished value of the AvMed services they received. Plaintiff Moore has also suffered actual damages in the amount of $4,298.77. Plaintiffs and members of the Classes have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
Negligence Per Se
(On Behalf of Plaintiffs and the Classes)

131. Plaintiffs repeat and re-allege all previous allegations as if fully set forth herein.

132. Defendant's violation of Fla. Stat. § 395.3025 resulted in injury to Plaintiffs and the Classes.

133. Fla. Stat. § 395.3025 was enacted to protect the confidentiality of medical information of Florida residents—such as Plaintiffs—and expressly provides that a person's medical information must not be disclosed without his or her consent. Fla. Stat. § 395.3025.

134. Defendant's disclosure of Plaintiffs' health information without authorization violates Fla. Stat. § 395.3025.

135. The disclosure of Plaintiffs' health information without authorization was the exact type of injury that Fla. Stat. § 395.3025 was designed to protect.

136. As a result of Defendant's conduct, Plaintiffs and members of the Classes have suffered actual identity theft. Plaintiffs 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; time spent scrutinizing bank statements, credit card statements, and credit reports; missed wages; expenses and/or time spent initiating fraud alerts; and, the diminished value of the AvMed services they received. Plaintiff Moore has also suffered actual damages in the amount of $4,298.77. Plaintiffs and members of the Classes have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VI
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Classes)

137. Plaintiffs repeat and re-allege all previous allegations as if fully set forth herein.

138. As guardians of Plaintiffs' and the members of the Classes' Sensitive Information, Defendant owed a fiduciary duty to Plaintiffs and the Classes to: (1) protect their Sensitive Information; (2) timely notify them of a data breach; and (3) maintain complete and accurate records of what and where its members' information is stored.

139. Defendant breached its fiduciary duty to Plaintiffs and the Classes by:

a. Failing to diligently investigate the data breach to determine number of members affected;

b. Failing to hire Price Waterhouse Coopers, or another forensics consultant, to investigate the number of members affected until February 2010 when the data breach occurred on December 10, 2009.

c. Failing to encrypt or otherwise protect the laptops containing Plaintiffs' and the Class members' and the Subclass members' Sensitive Information;

d. Failing to timely notify and/or warn Plaintiffs and the Class members and the Subclass members of the data breach;

e. Failing to ensure the confidentiality and integrity of electronic protected health information it created, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

g. Failing to implement technical policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility to maintain their security in violation of 45 CFR 164.310(d)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

i. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

j. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

k. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

l. Failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(94);

m. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502 et seq.;

n. Failing to effectively train all members of its workforce (including independent contractors involved in the data breach) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45CFR 164.308(a)(5);

o. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR164.530(c); and

p. Otherwise failing to safeguard Plaintiffs' and the Class members and the Subclass members' Sensitive Information.

140. As a result of Defendant's conduct, Plaintiffs and members of the Classes have suffered actual identity theft. Plaintiffs 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; time spent scrutinizing bank statements, credit card statements, and credit reports; missed wages; expenses and/or time spent initiating fraud alerts; and, the diminished value of the AvMed services they received. Plaintiff Moore has also suffered actual damages in the amount of $4,298.77. Plaintiffs and members of the Classes have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VII
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and the Classes)

141. Plaintiffs repeat and re-allege all previous allegations as if fully set forth herein.

142. In order to benefit from Defendant's healthcare plans, Plaintiffs and the Classes affirmatively assented to the provisions in the Defendant's service contracts.

143. The service contract provisions constitute a valid and enforceable contract between Plaintiffs and the Classes on the one hand, and Defendant on the other.

144. Defendant breached the provisions of its service contracts, specifically not honoring its responsibilities to ensure the "confidentiality of information about [members]' medical health condition being maintained by the Plan and the right to approve or refuse the release of member specific information including medical records, by AvMed, except when the release is required by law." (Ex. D).

145. Florida recognizes the implied covenant of good faith and fair dealing in every contract.

146. Implicit in the service contracts, were implied contract provisions that prevented Defendant from engaging in conduct that frustrated or injured Plaintiffs' and the Classes' rights to receive the benefits of the service contracts.

147. Defendant's obligation to follow HIPAA regulations and industry standards to safeguard and secure Plaintiffs' and the Classes' Sensitive Information from unauthorized access and theft was a material term of the service contracts. Defendant did not honor this obligation.

148. Defendant breached the implied covenant of good faith and fair dealing by failing to safeguard and secure Plaintiffs' and the members of the Classes' Sensitive Information from unauthorized access and theft, failing to promptly and sufficiently notify Plaintiffs and the members of the Classes that their Sensitive Information had been compromised, and further by failing to fully comply with the proscriptions of applicable statutory law.

149. As a result of Defendant's conduct, Plaintiffs and members of the Classes have suffered actual identity theft. Plaintiffs 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; time spent scrutinizing bank statements, credit card statements, and credit reports; missed wages; expenses and/or time spent initiating fraud alerts; and, the

diminished value of the AvMed services they received. Plaintiff Moore has also suffered actual damages in the amount of $4,298.77. Plaintiffs and members of the Classes have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class and Subclass, pray for the following relief:

A. Certify this case as a class action on behalf of the Class and Subclass as defined above, and appoint Juana Curry and William Moore as class representatives and undersigned counsel as lead counsel;

B. Find that AvMed is liable under all legal claims asserted herein for its failure to safeguard Plaintiffs' and Class members' Sensitive Information;

C. Find that AvMed's actions, as described herein, violate Fla. Stat. § 395.3025;

D. Award injunctive and other equitable relief as is necessary to protect the interests of the Classes, including: (i) an order prohibiting AvMed from engaging in the wrongful and unlawful acts described herein, and (ii) requiring AvMed to protect all data collected through the course of its business in accordance with HIPAA and industry standards;

E. Award damages, including statutory damages where applicable and punitive damages, to Plaintiffs and the Classes in an amount to be determined at trial;

F. Award restitution for any identity theft, including, but not limited to payment of any other costs, including attorneys' fees incurred by the victim in clearing

the victim's credit history or credit rating, or any costs incurred in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation of the victim arising as the result of Defendant's actions;

G. Award restitution in an amount to be determined by an accounting of the difference between the price Plaintiffs and the Classes paid in reliance upon Defendant's duty/promise to secure its members' Sensitive Information, and the actual services—devoid of proper protection mechanisms—rendered by Defendant;

H. Award Plaintiffs and the Classes their reasonable litigation expenses and attorneys' fees;

I. Award Plaintiffs and the Classes pre and post-judgment interest to the maximum extent allowable by law; and

J. Award such other and further legal or equitable relief as equity and justice may require.

JURY DEMAND

Plaintiffs request trial by jury of all claims that can be so tried.

Dated: April 25, 2011

JUANA CURRY AND WILLIAM MOORE
individually and on behalf of a class of similarly situated individuals

By: /s/ Steven W. Teppler
One of Their Attorneys

Jay Edelson
William C. Gray
Ari J. Scharg
Steven W. Teppler
Florida Bar No. 14787
EDELSON MCGUIRE, LLC
350 North LaSalle Street, Suite 1300
Chicago, Illinois 60654
Tel.: (312) 589-6470
Fax: (312) 589-6378

Edmund A. Normand
Florida Bar No. 865590
Diego M. Madrigal, III
Florida Bar No. 0037643
Wooten, Kimbrough, & Normand, P.A.
236 S. Lucerne Circle
Orlando, Florida 32801
Tel.: (407) 843-7060

CERTIFICATE OF SERVICE

I, STEVEN W. TEPPLER, HEREBY CERTIFY that, on April 25, 2011, I electronically filed the foregoing ***Second Amended Class Action Complaint***, with the Clerk of the Court using the CM/ECF system and served a copy of the foregoing by electronic mail on Defendant AvMed's counsel Paulo R. Lima, Esquire at plima@hunton.com, and John Delionado, Esquire, at jdelionado@hunton.com.

DEFENDANT'S COUNSEL:

Paulo R. Lima
Hunton & Williams
1111 Brickell Avenue, Suite 2500
Miami, FL 33131
Fax: 305-810-2460
Email: plima@hunton.com

John Delionado
Hunton & Williams
1111 Brickell Avenue, Suite 2500
Miami, FL 33131
Fax: 305-810-2460
Email: jdelionado@hunton.com