



their own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by their attorneys.

### **Parties**

1. Plaintiff Jean Resnick is a resident of Florida. She is a former customer of AvMed, Inc.'s services.

2. Plaintiff Miguel Vasquez is a resident of Florida. He is a customer of AvMed, Inc.'s services.

3. Plaintiff Christopher Atkinson is a resident of Florida. He is a customer of AvMed, Inc.'s services.

4. Plaintiff Rochel Albertson is a resident of Florida. She is a customer of AvMed, Inc.'s services.

5. Plaintiff Kirsten Atkinson is a resident of Florida. She is a former customer of AvMed, Inc.'s services and was a minor at the time of AvMed, Inc.'s data breach when her PHI was compromised.

6. Defendant AvMed, Inc. is a Florida corporation headquartered in Miami, Florida at 9400 South Dadeland Boulevard, Miami, FL 33156. AvMed does business throughout the State of Florida.

### **Jurisdiction and Venue**

7. Venue is properly laid in Dade County pursuant to section 47.051, Florida Statutes (2007) because Defendant conducts its regular business affairs through one or more agents or other representatives located in Dade County, Florida.

### **Conditions Precedent**

8. All conditions precedent have been performed or have occurred.


### **Conduct Complained Of**

#### **AvMed promises to secure highly confidential information that it receives from members.**

9. AvMed offers a variety of healthcare plans to both businesses and individuals throughout the State of Florida. In addition, AvMed offers Medicare plans to senior citizens.


10. Through its website, AvMed boasts of receiving awards for being among the top healthcare providers in the nation for financial strength and quality assurance.

11. AvMed asserts through its website that it will safeguard its members' highly confidential PHI. AvMed's Privacy Policy specifically states:

We follow the Health Insurance Portability  
and Accountability Act (HIPAA) Privacy  
Regulations to protect your personal health  
information. 

(See Exhibit A, attached hereto a true and accurate copy of AvMed's webpage entitled

"Protecting Your Privacy.")

12. The Privacy Policy also delineates member responsibilities. According to AvMed, members have a responsibility to "[p]rovide accurate and complete information about their health."  (Ex. A). Plaintiffs and the Class agreed to and complied with these terms and conditions.

13. When Plaintiffs and the Class agreed to subscribe and pay AvMed for its healthcare services, they relied upon AvMed's promise to safeguard their confidential information by following HIPAA regulations. AvMed demands that patients provide "accurate and complete information about their health." (Ex. A). In return, AvMed promises to keep that information safe. Members reveal highly sensitive and personal details about their health conditions to the company, and rely on AvMed to prevent that information from becoming public. AvMed members disclosed such private information because of AvMed's promises that it would be adequately guarded against exposure for the entire world to see.


14. Unfortunately for its members, and despite AvMed's promise to properly secure their members' PHI, a recent and devastatingly large data breach occurred. In fact, AvMed's data breach appears to be one of the largest recorded exposures of confidential medical data ever.

15. This data breach revealed that AvMed fails to take basic steps to keep patient information safe and does not honor their obligations to their customers.

16. Consequently, AvMed members are and remain vulnerable to potentially devastating acts of identity theft, as well as the publication of their highly confidential medical information.


**Unsecured and Unencrypted AvMed Computers containing members' PHI were easily stolen from AvMed offices.**

17. On or about December 10, 2009, two laptops were left unguarded in a conference room in AvMed's corporate office in Gainesville, Florida. Subsequently, the laptops containing the PHI were reported missing. Attempts to locate the stolen laptops have completely failed.

18. On or about December 23, 2009, AvMed officials determined that information contained on at least one of the laptops might not have been encrypted to prevent access to and widespread dissemination of AvMed members' PHI. 


19. AvMed's lapses in security extended not only to properly safeguarding their customers' PHI, but also in adequately understanding how many of its members were subjected to this devastating breach. Initially, AvMed believed that the laptops contained the confidential PHI of 208,000 AvMed members. Soon, that figure was increased to 360,000 members.

20. On or about February 5, 2009, AvMed publicly revealed the security breach and notified the 360,000 potentially affected members.

21. On or about June 3, 2010—one hundred and seventy-four (174) days after the initial breach was discovered—AvMed officials declared that they now believed an additional 860,000  current and former members' PHI might have been exposed as a result of the laptop theft. That figure also includes the PHI of dependents, *i.e.* the children of AvMed members.

22. In sum, the current total estimate of exposed PHI as a result of the security breach has now affected approximately 1.2 million current and former AvMed members.

**AvMed breaks its promise to its members by failing to safeguard their PHI.**

23. AvMed committed a wide variety of critical errors by storing unencrypted PHI on employee laptops and then leaving the computers within reach of any person with access to a conference room. Data encryption simply refers to an easy process that transforms plaintext into a form that is non-readable to unauthorized parties. Encryption is easily performed and often available at little, or even no cost. 

24. Essentially, by not encrypting members' PHI, *any person*, authorized or unauthorized, with access to one of these laptops could easily extract and misuse the highly

confidential data contained therein. Furthermore, storing such a substantial amount of sensitive data in one centralized location rather than compartmentalizing the data in various locations drastically increased the potential for a vast data breach like the one that AvMed allowed to occur.

25. As a result of AvMed's careless and reckless disregard for its members' PHI, 1.2 million persons have now been exposed to a wide variety of malicious activities. For example, a nefarious person who possesses this information could do any of the following:



(a) Use the Social Security Numbers and contact information contained on the laptop(s) to conduct full-scale identity theft, assuming the identity of any number of AvMed members;

(b) The buying and selling of United States citizens' identifications has become a prolific and lucrative business both domestically and abroad. Equipped with the PHI from the stolen laptops, a perpetrator now has 1.2 million identities to barter with;

(c) Apply for credit cards, bank accounts, or other credit extending services in the name of the members;

(d) Use the stolen, unencrypted PHI containing certain medical identification information to fraudulently apply for a healthcare plan;

(e) Post the highly confidential medical diagnosis information contained in the stolen files about any of the affected 1.2 million members. A perpetrator may publicly post this information on the Internet to humiliate AvMed members, or use the sensitive

information to extort or otherwise harass members<sup>1</sup>;

(f) Harvest the members' email addresses for spam. Assuming that each of the exposed members' email accounts is active, a spammer will have 1.2 million live email addresses to spam, as well the phone numbers contained in the records to use for spam text messages or for use in illegal phone bill cramming.

**Despite its assurances, AvMed does not follow HIPAA regulations.**

26. The Health Insurance Portability and Accountability Act ("HIPAA" or "the Act") was enacted in 1996. Title II of the Act 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 PHI, such as the data left unguarded by AvMed.

27. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA. For purposes of this Complaint, one of these rules is most significant: the Security Rule, which sets national standards for the security and confidentiality of electronic protected health information. <http://www.hhs.gov/ocr/privacy/>.

28. The Security Rule, codified at 45 C.F.R. § 164.302, *et seq.*, mandates that healthcare providers such as AvMed implement security measures to protect PHI.

29. Healthcare providers were required to comply with the Security Rule by April 20, 2005. <http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html>.

---


<sup>1</sup> In one such similar circumstance, extortionists attempted to elicit payments so that they would not reveal confidential prescription information. (See <http://www.washingtonpost.com/wp-dyn/content/article/2008/11/07/AR2008110703434.html>). Obviously, the exposure in the instant matter is much more potentially damaging given the astonishing breadth of the data stolen from AvMed.

30. The Security Rule is broken down into sections addressing administrative, physical, and technical safeguards. The general guidelines portion of the regulation states that healthcare providers must:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.


(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

45 C.F.R. §164.306(a).

31. As discussed *infra*, AvMed's  astounding practice of haphazardly leaving unencrypted PHI on laptops in an unattended conference room clearly violates the above guidelines. This failure is indicative of a systematic failure to protect against reasonably anticipated threats against the PHI it is legally obligated to safeguard.

**Administrative Safeguards, (45 C.F.R. § 164.308)**

32. The administrative safeguards provisions mandate that healthcare providers such as AvMed “[i]mplement policies and procedures to prevent, detect, contain, and correct security violations.” 45 C.F.R. § 164.308 (1)(i).

33. Importantly, this section of the Security Rule establishes that AvMed should implement procedures “to prevent those workforce members who do not have access [to  members’ PHI]” from viewing or accessing this very sensitive data. 45 C.F.R. § 164.308 (3)(i).

34. AvMed failed to properly implement policies, as commanded by HIPAA and the Security Rule, to ensure that workforce members without proper clearance could not access sensitive PHI. If AvMed had properly implemented the policies, laptops containing more than one million members' unencrypted PHI would not have been left unattended in a conference room.

35. Given that an unauthorized individual, quite possibly an AvMed employee without proper clearance, simply picked up the mobile, unlocked computing devices, the conclusion is clear. Either the HIPAA-mandated administrative safeguards, which AvMed promised to rigorously adhere to, were simply not implemented or they were implemented in such a way as to be rendered completely ineffectual.

36. Additionally, implicit in the provisions of the administrative safeguards are requirements that AvMed implement mechanisms to keep record of what PHI is stored and where it is stored. Because Defendant did not comply with these provisions, it took the company one hundred and seventy-four (174) days to determine that 860,000 members' unencrypted information was stored on a laptop. In other words, not only were 860,000 members exposed to terrible acts of identify theft, they were also wholly unaware of the data breach for several months and thus unable to take the proper steps to protect themselves.

37. On information and belief, AvMed failed to follow the administrative safeguards provisions of HIPAA as evidenced by the fact that laptops containing PHI were left in an unsecured location accessible to employees without proper access. In addition, it took AvMed several months to identify the members whose PHI was exposed as a result of the laptop theft because their information was not properly cataloged.

**Physical Safeguards, (45 C.F.R. § 164.310)**

38. Under the physical safeguards provisions, Defendant is obligated “to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.” 45 C.F.R. § 164.310 (a)(1).

39. Specifically, the rule’s standard compels AvMed to implement policies that control “the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.” 45 C.F.R. § 164.310 (d)(1).

40. A proper policy, compliant with the physical safeguards provisions designed to control the physical safeguarding of hardware and electronic media, would require that laptops containing unencrypted PHI be housed in a secure location. It is manifest that AvMed does not have such policies in place.

41. On information and belief, AvMed failed to adhere to the physical safeguards provisions of the Security Rule as evidenced by the company’s careless actions of leaving laptops containing unencrypted PHI unattended in a conference room.

#### **Technical Safeguards, (45 C.F.R. § 164.312)**

42. The technical safeguards of HIPAA compel healthcare providers to “maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.” 45 C.F.R. § 164.312 (a)(1).

43. This section of the Security Rule maintains that companies like AvMed should encrypt its members’ electronically stored PHI. 45 C.F.R. § 164.312 (a)(1)(iv). As discussed *supra*, the act of encrypting electronic data is now commonplace.

44. On information and belief, AvMed possessed the technical expertise to encrypt its members' highly confidential PHI, as evidenced by its December 23, 2009, statement that *at least* one laptop may not have been properly encrypted.

45. Despite its capacity to ensure members' confidentiality, AvMed chose not to encrypt PHI. As a result, AvMed's current and former members are now potential victims of the malicious activities described in paragraph 23.

**AvMed fails to comply with basic industry standards.**

46. In November of 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. 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>. On May 26, 2002, AES was adopted as the standard encryption technique of the United States federal government. *Id.* at ii. AES is free for any use private or public, commercial or non-commercial.

47. The NIST published a report in March of 2005 detailing methods for healthcare providers to comply with HIPAA's Security Rule.<sup>2</sup> In the Report, the NIST recommends specific techniques to safeguard electronically stored PHI. In one example, the NIST specifically recommends a system, easily implemented and maintained, to automatically encrypt PHI during non-work hours, and then decrypt it at the beginning of each workday. MATTHEW SCHOLL ET AL., NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEP'T OF

---

<sup>2</sup> An Introductory Resource Guide for Implementing the HIPAA Security Rule, [www.tulane.edu/~infosec/NIST/SP800-66.pdf](http://www.tulane.edu/~infosec/NIST/SP800-66.pdf) (revised in October, 2008) - <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>

COMMERCE. NIST SPECIAL PUBLICATION 800-66 REVISION 1, AN INTRODUCTORY RESOURCE GUIDE FOR IMPLEMENTING THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) SECURITY RULE, at 41 (2008), <http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>.

48. In light of the foregoing, it is obvious that AvMed has failed to comply with industry standards. Even more striking is that one of the exact example solutions recommended by the NIST, encrypting data during non-work hours, if implemented, would have almost certainly prevented the exposure of 1.2 million AvMed members' highly confidential information.

49. As the above discussion illustrates, AvMed has not only failed to comply with mandated HIPAA regulations, its actions egregiously departed from even basic industry standards.

#### **Amount In Controversy**

50. Plaintiffs make no specific allegation that the amount in controversy (including requests for attorneys' fees, injunctive relief, etc.) exceeds any specific amount, let alone \$5,000,000, other than meeting the jurisdictional requirements of this Court.

#### **The Facts Relating to Named Plaintiffs**

51. During the relevant time period, Jean Resnick, Miguel Vasquez, Christopher Atkinson, Rochel Albertson, and Kirsten Atkinson are or were AvMed members.

52. Jean Resnick, Miguel Vasquez, Christopher Atkinson, Rochel Albertson, and Kirsten Atkinson entrusted AvMed with their highly confidential PHI.

53. At the time of the breach Kirsten Atkinson was a minor.

54. Jean Resnick, Miguel Vasquez, Christopher Atkinson, Rochel Albertson, and Kirsten Atkinson received letters from AvMed informing them that their PHI had been compromised by a security breach. (*See* Exhibit B, attached hereto true and accurate copies of letters sent by AvMed to members concerning data breach of PHI).

### **Class Representation Allegations**

55. Plaintiffs bring this action on behalf of themselves and a class (the “Class”) defined as follows:

All individuals and entities in the United States that are current or former members of healthcare plans provided by AvMed, Inc. and had their PHI compromised through the theft of AvMed laptops.

Excluded from the Class 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 Class; 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 AvMed’s laptops.

56. This action is suitable for class treatment pursuant to Florida Rule of Civil Procedure 1.220(b)(2).

57. **Numerosity:** The exact number of Class members is unknown to Plaintiffs at this time, but on information and belief, there are at least 1.2 million members of this Class

throughout the country, making joinder of each individual member impracticable. Ultimately, the Class members will be easily identified through Defendant's records.

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

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

60. **Appropriateness:** 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 Class is impracticable. The damages suffered by the individual members of the Class 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 Class to obtain effective relief from Defendant's misconduct. Even if members of the Class 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 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.

61. **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 Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply and affect members of the Class uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

62. **Commonality and Predominance:** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual members:

- (a) Whether AvMed failed to use reasonable care and/or comply with HIPAA and applicable industry standards to secure and safeguard its members' highly confidential PHI;
- (b) Whether storing member PHI in an unencrypted format was reasonable under industry standards;
- (c) Whether leaving laptops containing highly confidential PHI unattended in a conference room was reasonable under industry standards;
- (d) Whether AvMed's conduct described herein violated the Florida Statute Prohibiting Misleading Advertising (Fla. Stat. § 817.41);
- (e) Whether AvMed's conduct described herein constitutes a breach of contract;
- (f) Whether AvMed's conduct described herein constitutes breach of the

implied covenants of good faith and fair dealing;

(g) Whether AvMed's conduct described herein constitutes breach of implied contracts;

(h) Whether AvMed's conduct described herein was negligent and/or grossly negligent; and

(i) Whether AvMed's conduct described herein constitutes negligence per se.

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

### **COUNT I**

#### **Violation of the Florida Statute Prohibiting Misleading Advertising (§ 817.41 *et seq.*) (On Behalf of Plaintiffs and the Class)**

64. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

65. AvMed has disseminated a misleading advertisement to the general public in violation of Fla. Stat. § 817.41(1).

66. As discussed above, AvMed publicly advertises through its website, and likely in various other documents, that it follows HIPAA regulations to protect its members' PHI. (Ex. A). AvMed's recent data breach reveals that HIPAA regulations are not in fact being followed, therefore these advertisements are misleading.

67. Plaintiffs and the Class members relied on AvMed's misleading advertising, and have suffered irreparable injury as a result of Defendant's unlawful conduct, including the theft of their highly confidential PHI. Additionally, because the stolen information cannot be returned, the harm from the security breach is ongoing and compounding. Accordingly, Plaintiffs and the Class are entitled to maximum relief, including punitive damages, under § 817.41(6).

### **COUNT II**

**Breach of Contract  
(On Behalf of Plaintiffs and the Class)**

68. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

69. Defendant asserts through its website certain contractual agreements (“the Agreement”) that bind both AvMed and its members. That Agreement provides reciprocal responsibilities that AvMed requires the Plaintiffs and the Class to affirmatively assent. Particularly, the Agreement requires AvMed members to “[p]rovide accurate and complete information about their health.” In turn, AvMed promises to “follow the Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations to protect your personal health information.” (Ex. A).

70. The Agreement’s provisions constitute a valid and enforceable contract between Plaintiffs and the Class on the one hand, and Defendant on the other.

71. Plaintiffs and the Class performed all of their obligations under the Contract.

72. Defendant materially breached the terms of the Agreement by its wrongful conduct alleged herein, including failing to properly secure its laptops and the PHI contained therein. As a result, the Plaintiffs’ and the Class’s sensitive PHI was exposed.

73. As a result of Defendant’s misconduct and breach of the Agreement described herein, Plaintiffs and the Class suffered injury.

**COUNT III  
Breach of the Implied Covenant of Good Faith and Fair Dealing  
(On Behalf of Plaintiffs and the Class)**

74. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

75. In order to benefit from Defendant's healthcare plans, Plaintiffs and the Class affirmatively assented to the provisions in the Defendant's Agreement.

76. The Agreement's provisions constitute a valid and enforceable contract between Plaintiffs and the Class on the one hand, and Defendant on the other.

77. Defendant breached the provisions of its Agreement, specifically not honoring its responsibilities to ensure in 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. A).

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

79. Implicit in the Agreement, along with the explicit provisions, were contract provisions that prevented Defendant from engaging in conduct that frustrated or injured Plaintiffs' and the Class's rights to receive the benefits of the Agreement.

80. Defendant's obligation to follow HIPAA regulations and industry standards to safeguard and secure Plaintiffs' and the Class's highly confidential PHI from unauthorized access and theft was a material term of the Agreement. Defendant did not honor this obligation.

81. Furthermore, implicit in the terms of the Agreement was Defendant's obligation to be truthful in its advertisements as mandated by the Florida Statute Prohibiting Misleading Advertising (§ 817.41 *et seq.*).

82. Defendant breached the implied covenant of good faith and fair dealing by failing to safeguard and secure Plaintiffs' and the Class's sensitive PHI from unauthorized access and theft, failing to promptly and sufficiently notify Plaintiffs and the Class that their sensitive PHI

had been compromised, and further by failing to fully comply with the proscriptions of applicable statutory law.

83. Defendant's misconduct and breach of the implied covenant of good faith and fair dealing as described herein resulted in injury to Plaintiffs and the Class.

**COUNT IV**  
**Breach of Implied Contracts**  
**(On Behalf of Plaintiffs and the Class)**  
**(In the Alternative)**

84. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

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

86. By providing that highly sensitive PHI and upon Defendant's acceptance of such information, Plaintiffs and the Class, on the one hand, and Defendant, on the other hand, entered into implied contracts whereby Defendant was obligated to take reasonable steps mandated by state and federal statutes as well as industry standards to secure and safeguard that information.

87. Under the implied contract, Defendant was further obligated to provide Plaintiffs and the Class prompt and sufficient notice of any and all unauthorized access and/or theft of their sensitive PHI.

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

89. By failing to properly secure Plaintiffs' and the Class's highly confidential PHI, and further by failing to promptly notify Plaintiffs and the Class that their personal information had been compromised, Defendant breached its implied contracts with Plaintiffs and the Class.

90. Defendant's breach and other misconduct described herein resulted in injury to Plaintiffs and the Class.

**COUNT V**  
**Negligence**  
**(On Behalf of Plaintiffs and the Class)**

91. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

92. In order to benefit from Defendant's healthcare plans, Plaintiffs and the Class disclosed highly confidential information to AvMed.

93. By agreeing to accept Plaintiffs' and the Class's sensitive PHI, Defendant assumed a duty, which required it to exercise reasonable care to secure and safeguard that information and to utilize reasonable methods to do so.

94. Defendant failed to protect its members' PHI and failed to provide Plaintiffs and the Class with prompt and sufficient notice that their sensitive PHI had been compromised, thereby breaching its duties to Plaintiffs and the Class.

95. By failing to take proper security measures to protect Plaintiffs' and the Class's sensitive PHI as described herein, Defendant's conduct was grossly negligent and departed from all reasonable standards of care.

96. As a direct and proximate result of Defendant's failure to exercise reasonable care and comply statutorily mandated and industry standards reasonable security measures, its

members' highly confidential PHI was accessed without authorization and Plaintiffs' and the Class's sensitive PHI was exposed.

97. That security breach and resulting unauthorized access to Plaintiffs' and the Class's sensitive PHI was reasonably foreseeable by Defendant, particularly in light of the fact that AvMed possessed the technical expertise to implement proper encryption and physical protection mechanisms.

98. Neither Plaintiffs nor the other members of the Class contributed to the security breach described herein or to the unauthorized access of their sensitive PHI.

99. AvMed's reckless indifference to the proper security measures necessary to protect its users' sensitive PHI created the gaping security lapses necessary for a malicious third party to directly access its members' highly confidential PHI. Without AvMed's reckless and/or gross negligence and unwillingness to follow statutorily-set standards and industry standards for data security it claims to adhere to, a third party could not have stolen Plaintiffs' and the Class's sensitive PHI.

100. As a direct and proximate result of Defendant's misconduct described herein, Plaintiffs and the Class were injured.

**COUNT VI**  
**Negligence Per Se**  
**(On behalf of Plaintiffs and the Class)**

101. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

102. Defendant's violation of Fla. Stat. § 817.41 resulted in injury to Plaintiffs and the Class.

103. The harm Defendant caused to Plaintiffs and the Class are injuries that result from the type of occurrences those statutes were designed to prevent.

104. Plaintiffs and the Class are the type of persons for whose protection those statutes were adopted.

105. Defendant's violations of the foregoing statutes as described herein resulted in injury to Plaintiffs and the Class.

### **PRAYER FOR RELIEF**

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

A. Certify this case as a class action on behalf of the Class defined above, appoint Jean Resnick, Miguel Vasquez, Christopher Atkinson, Rochel Albertson, and Kirsten Atkinson as class representatives, and appoint their counsel as class counsel;

B. Declare that AvMed's actions, as described herein, violate the Florida Statute Prohibiting Misleading Advertising (§ 817.41 *et seq.*);

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including, *inter alia*: (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;

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

E. Award restitution for any identity theft, including but not limited to payment of any other costs, including attorney's 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 the actions of the defendant.

F. Award Plaintiffs and the Class their reasonable litigation expenses and attorneys' fees;

G. Award Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and

H. Award such other and further relief as equity and justice may require.

### **JURY DEMAND**

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

November \_\_\_\_, 2010

Jean Resnick, Miguel Vasquez, Christopher Atkinson, Rochel Albertson, and Kirsten Atkinson individually and on behalf of a class of similarly situated individuals

---

Counsel to Plaintiffs

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

Firm ID: 44146

\*Pro hac vice admission to be sought

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

Fax: (407) 843-5836