

## Notification Letter to Affected Individuals

Protecting the privacy of personal information is a critical priority at AvMed Health Plans. This notice contains details about a matter involving the personal information of some current and former AvMed members.

In December 2009, two company laptop computers were stolen from one of AvMed's corporate buildings in Gainesville, Florida. We promptly reported the theft to law enforcement authorities and began an investigation. We notified some of our current and former members that, as a result of the theft, there was a possible compromise of their information, including names, addresses, dates of birth, Social Security numbers and health-related information. As our investigation has progressed, we now have reason to believe that additional individuals' information also may have been on the laptops. We are notifying those individuals by mail.

AvMed takes the privacy of our members' information very seriously and we deeply regret any inconvenience or concern this matter may cause. While we have no evidence that any personal information has been misused as a result of this incident, there are steps affected individuals may take to help protect themselves. We encourage affected individuals to remain vigilant and regularly review and monitor their credit reports. We also recommend regularly reviewing medical bills (including "Explanation of Benefits" statements) to check for inaccurate or unauthorized charges. The Reference Guide below provides details on steps affected individuals may wish to consider, including recommendations by the U.S. Federal Trade Commission on how to further protect against identity theft, and information on how to place a fraud alert or security freeze on a credit file.

To further assist affected individuals, AvMed has arranged to provide two years of identity protection under the Debix Identity Protection Network at no cost to individuals who receive a notification letter from AvMed. If the individual who receives a letter is under the age of eighteen, AvMed has arranged to provide two years of identity protection services with Debix ChildScan.

If you have questions regarding this incident, please call 877-441-3004 toll-free for additional information. Representatives are available Monday through Saturday, 10 a.m. to 8 p.m. EDT. TTY users should call 877-442-8633.

Please be assured that we are taking steps to enhance our security and help ensure that this type of incident does not happen in the future.

Sincerely,

A handwritten signature in cursive script that reads "Ed Hannum".

Edwin Hannum  
President

## Reference Guide

We encourage affected individuals to take the following steps:

**Order Your Free Credit Report.** You are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call 877-322-8228 toll-free, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC's) website at [www.ftc.gov](http://www.ftc.gov) and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information, such as home address and Social Security number. If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft.

You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. If you find items you don't understand on your report, call the credit bureau at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

**U.S. Federal Trade Commission Recommendations.** If you detect any unauthorized transactions in your financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
<http://www.ftc.gov/idtheft/>

**Place a Fraud Alert on Your Credit File.** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with all three credit bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	877-478-7625	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

**Place a Security Freeze on Your Credit File.** You may wish to place a “security freeze” on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit report at the three national credit bureaus without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from \$5-\$20 per action. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. Since the instructions for how to establish a security freeze differ from state to state, please contact the three national credit bureaus to find out more information. The credit bureaus may require that you provide proper identification prior to honoring your request.

Equifax	P.O. Box 105788 Atlanta, Georgia 30348	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	www.transunion.com