



RECEIVED  
OFF OF THE ATTY GENERAL  
2008 JAN 23 P 3: 05

Devin Ehrlich  
Executive Vice President,  
General Counsel  
678-443-6772 (Direct)  
678-443-6874 (Fax)  
dehrlich@marinerhealthcare.com

January 18, 2008

Hon. Douglas F. Gansler  
Office of the Maryland Attorney General  
200 St. Paul Place  
Baltimore, Maryland 21202

**Re: Notice of Breach of Security**

Dear Attorney General Gansler:

This letter is to notify you that Mariner Health Care, Inc. ("Mariner") has experienced a breach of security involving the personal information of employees and former employees of Mariner and its affiliates that are eligible to participate in Mariner's 401(k) benefit plan. Mariner has conducted an investigation of this breach and, to date, is aware of no evidence that the personal information of any individual actually was compromised or misused. Nevertheless, in an abundance of caution, Mariner is sending notice of this breach to affected individuals, including 2,199 Maryland residents, advising these individuals of the breach and steps that they can take to prevent and detect identity theft.

On the evening of December 31, 2007, the offices of Windham Brannon, P.C. ("Windham") in Atlanta, Georgia were burglarized and several laptop computers were stolen, as well as some amount of cash. Windham provides audit services for Mariner's 401(k) benefit plans, and one of the stolen computers, which was password protected, contained unencrypted personal information about Mariner employees and former employees. Windham discovered the theft on January 2, 2008 and reported it to the Atlanta Police Department. Windham notified Mariner of the incident on January 4.

The stolen computer that contained information about Mariner employees and former employees was recovered by the Atlanta Police Department on January 7, 2008 and was returned to Windham on the following day. Through its counsel, Mariner then engaged forensic computer examiners at Navigant Consulting to inspect the computer in an effort to determine whether any files containing personal information had been accessed. Windham made the laptop available to the examiners on January 9, and the



Hon. Douglas F. Gansler

Page 2

January 18, 2008

examiners conducted their analysis on January 10 and 11. The examiners found that the computer was reformatted within a few hours of the theft and that, as a result, most of the files containing personal information about Mariner employees and former employees had been destroyed. Consequently, the examiners were not able to determine with certainty whether these files were accessed before they were destroyed. However, the examiners were able to find three of our files that had not been over-written and determined that these files had not been accessed after the theft. The examiners also inspected the data files of other clients' that survived the reformatting process and determined that none of these files were accessed at any time after the theft.

These circumstances lead us to believe that the personal information of Mariner employees and former employees was not a target of the burglary and likely has not been compromised or misused. Nevertheless, because Mariner cannot be certain, we are sending notice to all individuals whose personal information was contained on the laptop at the time of the theft. This notice will be sent to the individuals by mail beginning on January 18, 2008. A copy of the notice that will be sent to Maryland residents is attached. We also have contacted Fidelity, which maintains our employees and former employees' 401(k) accounts, and informed Fidelity of the breach. In addition, we will be reporting the breach to the three national consumer credit reporting agencies.

Please contact me if you require additional information.

Very truly yours,

Devin Ehrlich  
Executive Vice President, General Counsel

Enclosures



January 18, 2008

**NOTICE OF SECURITY BREACH  
INVOLVING YOUR PERSONAL INFORMATION**

We are writing to inform you of a security breach involving your personal information.

We recently received notice that several laptop computers were stolen on December 31, 2007 from the offices of an accounting firm that provides audit services for our 401(k) benefit plan. One of these laptops contained sensitive information concerning our 401(k) plan, including your name, home address, social security number, and date of birth. This laptop also may have contained your salary, 401(k) account number, and 401(k) balance information. The password to access your 401(k) account was not contained on the laptop. Although the laptop was password protected, the information stored on it was not encrypted.

The theft was reported to local law enforcement officials, who recovered the laptop that contained your personal information on January 7, 2008. After the laptop was recovered, we engaged forensic computer examiners to determine if any files on the laptop had been accessed. In the course of their investigation, these examiners found that the laptop had been reformatted within hours of the theft and that, as a result, substantially all of the files containing your personal information were destroyed. The examiners also inspected files on the laptop that survived the reformatting process and determined that none of these files were accessed after the theft. Although we cannot be certain that files were not downloaded or copied before the laptop was reformatted, we have no evidence at this time indicating that your personal information has been misused, accessed, or retained by unauthorized persons.

Because there is some risk that your personal information has been compromised and could be misused, you should be vigilant for suspicious activity concerning your identity and financial and credit accounts. We have notified Fidelity, our 401(k) plan administrator, of this security breach, and Fidelity has informed us that, to date, no suspicious activity has been reported to Fidelity concerning our 401(k) plan. Nevertheless, we recommend that you access your 401(k) account and change your password immediately.

There are other steps that you can take to minimize any potential risk of identity theft. The Federal Trade Commission recommends, among other things, that you review your credit reports for unusual activity. Under federal law, you are entitled each year to Report Request Service, P.O. Box 105281, Atlanta, Georgia 30348-5281. You also should review your financial account and billing statements carefully for unusual activity.



Page 2  
January 18, 2008

one free copy of your credit report from the three national consumer credit reporting agencies. To request a copy of your credit report, visit <http://www.annualcreditreport.com>, call 1-877-322-8228, or write to Annual Credit

If you detect suspicious activity, the Federal Trade Commission recommends that you contact one of the three national consumer credit reporting agencies and request that they place a "fraud alert" on your credit file. A fraud alert directs creditors to follow certain procedures before they open new accounts in your name or modify your existing accounts. You can contact the national consumer credit reporting agencies as follows:

Equifax (888) 766-0008 <a href="http://www.equifax.com">http://www.equifax.com</a> P.O. Box 740241 Atlanta, GA 30374-0241	Experian (888) 397-3742 <a href="http://www.experian.com">http://www.experian.com</a> P.O. Box 9532 Allen, TX 75013	TransUnion (800) 680-7289 <a href="http://www.transunion.com">http://www.transunion.com</a> P.O. Box 6790 Fullerton, CA 92834-6790
---	---	--

In some states, you also may have a right to request a "credit freeze," which requires the use of a personal identification number issued to you at the time you request the freeze to open any new credit account. Procedures for requesting a credit freeze may vary from state to state, and there may be fees for placing, lifting, or removing a credit freeze. For more information, contact the national consumer credit reporting agencies.

Finally, if you have reason to believe that you are a victim of identity theft, you also should report the matter to appropriate law enforcement agencies, including the Federal Trade Commission, and to us.

For more information on steps that you can take to prevent and detect identity theft, you can contact the Federal Trade Commission or the Office of the Maryland Attorney General as follows:

Federal Trade Commission (877) 438-4338 <a href="http://www.ftc.gov/">http://www.ftc.gov/</a> 600 Pennsylvania Avenue, N.W. Washington, D.C. 20580	Maryland Attorney General (888) 743-0023 <a href="http://www.oag.state.md.us/">http://www.oag.state.md.us/</a> 200 St. Paul Place Baltimore, MD 21202
--	---



Page 3  
January 18, 2008

If we subsequently learn that your personal information, in fact, was accessed by unauthorized persons, we will contact you and provide you with additional details. If you have any questions, we have set up a toll-free number for you to contact us at (866) 273 - 6122.

Sincerely,

Kim L. Pennock  
Employee Relations