



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

January 18, 2008

Hon. Martha Coakley
Office of the Attorney General
One Ashburton Place
Boston, Massachusetts 02108

Director Daniel Crane
Office of Consumer Affairs and Business Regulation
Ten Park Plaza, Suite 5170
Boston, Massachusetts 02116

Re: Notice of Breach of Security

Dear Attorney General Coakley and Director Crane:

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 283 Massachusetts 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 plan, 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



Hon. Martha Coakley
Director Daniel Crane
Page 2
January 18, 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 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 Massachusetts 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,

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 a data storage device containing your personal information, including your name, home address, social security number, and date of birth, and possibly your salary, 401(k) account number, and 401(k) balance information, was stolen from an outside auditor. The device subsequently was recovered. We have conducted an investigation of the security breach and, although we cannot be certain whether files containing your information were accessed or copied by unauthorized persons, we have no evidence at this time indicating that your personal information, in fact, was improperly accessed or otherwise misused.

Because there is some risk that your personal information has been compromised, 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 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 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 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.

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
<http://www.equifax.com>
P.O. Box 740241
Atlanta, GA 30374-0241

Experian
(888) 397-3742
<http://www.experian.com>
P.O. Box 9532
Allen, TX 75013

TransUnion
(800) 680-7289
<http://www.transunion.com>
P.O. Box 6790
Fullerton, CA 92834-6790



Page 2
January 18, 2008

For more information on steps that you can take to prevent and detect identity theft, visit the website of the Federal Trade Commission at <http://www.ftc.gov>.

In Massachusetts, you also have a right to request a "security 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. To place a security freeze on your credit report, send a request in writing, by mail, to each of the three credit reporting agencies listed above and include the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.), address, social security number, and date of birth;
- If you have moved in the past five years, the addresses where you have lived over the prior five years;
- Proof of current address (e.g., current utility bill or phone bill);
- Photocopy of a government issued identification card (e.g., state driver's license or ID card, military identification, etc.); and
- If you are a victim of identity theft, a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft; or
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, Master Card, American Express, or Discover) in the amount of \$5.

The credit reporting agencies are not allowed to charge a fee to Massachusetts residents who are victims of identity theft, or their spouses, for placing, removing a security freeze for a specific period or party, or removing a security freeze on a credit report. Other consumers are required to pay a \$5 fee for placing, temporary lifting, or removing a security freeze and should send payment to the credit reporting agencies by check, money order, or by credit card.

If you believe that you are the victim of identity theft, you should report the matter to appropriate law enforcement agencies, including the Federal Trade Commission, and to us. Under Massachusetts law, if you are a victim of identity theft, you have a right to obtain a police report.

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