Harvard Pilgrim Health Care

VIA OVERNIGHT MAIL

January 21, 2015

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of Breach of Personal Information

Dear Sir or Madame:

Pursuant to N.H. Rev. Stat. Ann. §§ 359-C:20, I am writing to you on behalf of Harvard Pilgrim Health Care, Inc. (Harvard Pilgrim) to notify you of a breach of personal information involving seven New Hampshire residents.

Nature of the Security Breach

On December 10, 2014, a Harvard Pilgrim laptop was stolen from the Massachusetts home of a Harvard Pilgrim employee between the hours of 10am and 1pm. When the employee returned home and discovered the theft, she called the police and filed a police report. On the same day, the employee notified her supervisor at Harvard Pilgrim who in turn notified Harvard Pilgrim's Office of Information Security.

Within hours of being notified of the theft, Harvard Pilgrim's Office of Information Security determined that this particular laptop was not running encryption software. Encryption software is standard on all of Harvard Pilgrim's laptops and desktops. While the encryption software on this particular laptop was deployed, it had not properly installed. The reason that the encryption software had not installed on the stolen laptop is likely due to a conflict between software installations that were attempting to run concurrently at the time the laptop was deployed to the employee. Although the encryption software was not installed, the laptop was properly password protected. We have no reports that the personal information located on the laptop has been accessed or misused.

The employee was authorized to use her laptop at home. As part of her responsibilities, the employee handles personal information in the form of emails, faxes, claim forms and access to Harvard Pilgrim's member management system. The electronic personal information involved in this incident included the individual's first and last name and Social Security number.

Number of New Hampshire Residents Affected

A total of seven (7) New Hampshire residents had personal information that may have been exposed as a result of this incident. All of the impacted individuals have been sent a letter

Harvard Pilgrim Health Care, Inc.
93 Worcester Street, Suite 100
Wellesley, Massachusetts 02481

pursuant to N.H. Rev. Stat. Ann. §§ 359-C:20 notifying them of the incident. Those notices were mailed between December 22, 2014 and December 29, 2014. I have enclosed a sample copy of the notice to impacted New Hampshire residents with this letter.

Steps Harvard Pilgrim Has Taken Related to the Incident

After discovering that the stolen laptop was not running encryption software, Harvard Pilgrim's Office of Information Security took the following steps. On the same day the theft occurred, Harvard Pilgrim ran a series of assessments to determine whether any other laptops or desktops did not have encryption software properly installed and running. Out of over 2,000 Harvard Pilgrim computers, we identified thirty-nine computers on which encryption software was deployed but was not installed. Within 24 hours of receiving the initial report of the theft, Harvard Pilgrim had successfully installed encryption software on all of those thirty-nine computers.

As a next step, Harvard Pilgrim developed multiple processes intended to run side-by-side to ensure that encryption software is properly installed on all of our computers. First, our information technologists created a report that automatically runs every morning at 7am. This report identifies any computer that does not have encryption software installed. If a computer is identified, the encryption software will be manually installed on such computer and we will verify that it is running properly. In addition, our information technologists added a function to Harvard Pilgrim's asset management system that automatically installs encryption software if the asset management system determines that it is not installed on a particular device. These steps are meant to build in redundancy to better ensure that encryption software is installed on all laptops and desktops.

In addition to the steps above, Harvard Pilgrim has developed multiple fail-safe procedures to ensure that (1) we have an accurate count of all active laptops and desktops, and (2) that encryption software is running on these computers.

As stated above, we have no evidence that any of the personal information that was on the laptop has been either accessed or misused. The theft was reported to the police when the employee discovered it.

Harvard Pilgrim has offered free credit monitoring and credit restoration services to all impacted residents for one year. Those individuals were informed of how they can activate their credit monitoring services in the notification letter they received (sample copy attached).

Contact Information

If you have additional questions or need further information, please contact me at [redacted]

Sincerely,

[redacted]

Enclosure

cc: Commissioner of the New Hampshire Insurance Department

Harvard Pilgrim Health Care

<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

Dear <<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>,

We are writing to notify you about a security incident that may have exposed your personal information, including your name, Social Security number, date of birth, Harvard Pilgrim membership number, address, telephone number, provider, dates of service and procedure descriptions. The incident, which involved the theft of a laptop from an employee's home, occurred on December 10, 2014.

We want to apologize to you and help alleviate concerns you may have about this incident. First, Harvard Pilgrim Health Care takes confidentiality seriously. Maintaining your privacy is one of our highest priorities. We have taken steps to address and correct this situation and to prevent it from happening again.

We are also offering identity theft protection services to you, paid for by Harvard Pilgrim. Harvard Pilgrim has secured the services of Kroll to provide credit monitoring and identity theft consultation and restoration at no cost to you for up to one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential information. Please note that in order to activate these services you will need to follow the instructions in the section titled "How to Take Advantage of Your Identity Theft Protection Services" below. To receive credit monitoring, you must be over the age of 18, have established credit in the U.S., have a Social Security number, and have a U.S. residential address.

Harvard Pilgrim strives to meet the expectations of our members. We again apologize for any inconvenience or concern this has caused you. If you have any further questions, please contact me at Harvard Pilgrim by calling 888-333-4742.

Sincerely,

Maria L Fitzgerald

Maria Fitzgerald
Director of Member Services

How to Take Advantage of Your Identity Theft Protection Services from Kroll

Visit krollbreach.idMonitoringService.com and follow the online instructions to take advantage of your identity theft protection services.

You can view your services at any time by logging onto Kroll's identity protection website. When you enroll, be prepared to provide your membership number.

krollbreach.idMonitoringService.com is compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox or Safari.

Membership Number: <<Member ID>>

Help is only a phone call away.

If you have a question, need assistance, or feel you may be a victim of identity theft, Call 1-866-775-4209, 8 a.m. to 5 p.m. (Central Time), Monday through Friday, and ask to speak with an investigator.

Take advantage of this no-cost opportunity and let the experts at Kroll help you assess your situation and safeguard your identity.

To receive your credit services by mail instead of online, please call 1-844-263-8605.

974R87-1214

Kroll

Take Advantage of Your Identity Theft Protection Services

You've been provided with access to services from Kroll, a global leader in risk mitigation. Over the past 14 years, Kroll has provided data breach response services for cases impacting more than 100 million individuals including personal consultation to more than 180,000 consumers and worked some 8,000 confirmed identity theft cases. When you need assistance, rest assured that your services are backed by an expert team who can answer any question you may have.

The following services are included in your **Credit Monitoring** package:

Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

Consultation: You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Restoration: Kroll's restoration services are the most comprehensive of any provider. Should you become a victim of identity theft, a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and more ... to resolve it.

Credit Monitoring: Credit monitoring can be a key tool in detecting early warning signs of identity theft. You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of identity theft. You'll also receive "no activity" notices if there have been no changes to your data.

How to Take Advantage of Your Identity Theft Protection Services

Visit krollbreach.idMonitoringService.com and follow the online instructions to take advantage of your identity theft protection services.

You can view your services at any time by logging onto Kroll's identity protection website. When you enroll, be prepared to provide the membership number included with the accompanying letter.

Help is only a phone call away.

If you have a question, need assistance, or feel you may be a victim of identity theft, call Kroll at the toll-free number provided in the accompanying letter, and ask to speak with an investigator.

Take advantage of this no-cost opportunity and let the experts at Kroll help you assess your situation and safeguard your identity.

krollbreach.idMonitoringService.com is compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox or Safari.