Weyerhaeuser

SUSTAINABLE FORESTRY INITIATIVE

Corporate Headquarters • PO Box 9777 • Federal Way, WA 98063-9777

15 APR -6 PM 3:4[illegible]

CONSUMER PROTECTION DIV.

April 2, 2015

The Honorable Tom Miller
Attorney General of Iowa
Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319

Regarding: Follow-up letter regarding Premera Blue Cross security breach

Dear Mr. Attorney General:

Weyerhaeuser Company is providing letters to each Weyerhaeuser enrollee in a Premera Blue Cross health plans that has been identified by Premera as having personal information accessed during the breach of Premera's IT systems.

According to Premera, the breach started as early as May of 2014 and was discovered on January 29, 2015. Premera notified Weyerhaeuser on March 17th of 2015. Additional details about the breach are in the sample letter which is attached.

Premera has told Weyerhaeuser that it is providing letters to the Weyerhaeuser enrollees, however, Weyerhaeuser is providing letters to our enrollees to make sure they are notified and to provide them with additional information to protect themselves from fraudulent activities.

Please contact me if you have additional questions or concerns.

Best regards,

Teresa J. Wiant
Senior Intellectual Property Counsel
Weyerhaeuser NR Company
Teresa.Wiant@Weyerhaeuser.com

Attachment

Weyerhaeuser

March __, 2015

_____

Dear _____

This letter is to provide you notice on behalf of Weyerhaeuser that your personal information may have been affected by the Premera Blue Cross security breach.

WHAT HAPPENED?
On March 17, 2015, Premera notified Weyerhaeuser and others that cyber-attackers had gained unauthorized access to Premera's Information Technology (IT) systems since as early as May of 2014. Premera discovered the unauthorized access on January 29, 2015. Premera's investigation determined that the attackers may have gained unauthorized access to information on Weyerhaeuser enrollees in Premera health plans, dating back to 2005. Premera says the information accessed may include name, date of birth, address, email address, telephone number, Social Security number, member identification number, and claims information, including clinical information.

Premera says it has no evidence at this time that any data was removed at any point during this security breach of Premera's IT systems. Premera also says it has no evidence such data has been used inappropriately since the security breach of Premera's IT systems. However, because personal information may have been accessed, Premera also began mailing letters to affected individuals on March 18, 2015. Premera has also indicated that it has cleansed its IT systems and taken steps to strengthen and enhance its security going forward.

WHY ARE YOU RECEIVING THIS LETTER?
Premera gave us your name as an individual whose information may have been accessed in this incident. Premera began mailing notification letters to affected members on March 18, 2015. If you do not receive a letter from Premera, please contact Premera at **1-800-768-5817**. Premera is also doing the following:

- **Offering Free Credit Monitoring:** Premera will offer two years of free credit monitoring and identify-theft protection services to anyone affected by this incident. You can enroll in this service in advance of receiving notification from Premera by going to http://premeraupdate.com/free-credit-monitoring/
- **Posting Updates Online:** Information about this incident is posted at www.premeraupdate.com.
- **Answering Questions:** Call Premera with any questions you have at **1-800-768-5817** weekdays from 5 a.m. to 8 p.m. Pacific time.

HOW TO PROTECT YOURSELF FROM FRAUD

1. **Get Updates:** Visit www.premeraupdate.com for accurate up-to-date information.

2. **Vigilance:** We recommend that you be vigilant about reviewing your financial account statements and Explanations of Benefits, and routinely monitor your credit report for any fraudulent activity.

3. **Get Free Monitoring:** Take advantage of the free credit monitoring and identity-theft protection that Premera is offering.

4. **Place a fraud alert:** Consider placing a "fraud alert" on your records with credit reporting companies. This will require credit reporting companies to take extra precautions if they are contacted about you by others. The three major credit reporting companies are Equifax, Experian, and TransUnion.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-EXPERIAN (397-3742)	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834-6790

5. **Don't fall for scams:** Be alert for potential scam emails, phone calls and letters that may ramp up in the wake of this incident. Premera says it will not email you or make unsolicited phone calls to you about this data security breach. Regardless of this situation, you should never provide personal information in response to emails or phone calls for any reason, no matter how convincing they may seem.

6. **Watch for tax fraud:** Be alert when filing your income tax returns. With the types of data that were exposed, it is possible for these cyber-criminals to file a fraudulent income tax return in your name. If a fraudulent return is filed before you file your income tax return, your return may be rejected and you will need to work with the IRS to prove that the other return was fraudulent.

7. **Request a credit report annually:** Under federal law, the three major credit reporting companies mentioned above are each required to provide you with a free copy of your credit report once per year. You can contact those companies directly or go to www.AnnualCreditReport.com.

8. **Visit the Federal Trade Commission website or the Attorney General website in your state:** Additional information about protecting yourself against fraud and identity theft can be found at http://www.consumer.ftc.gov/features/feature-0014-identity-theft or at the website of your state's Attorney General. You can also contact the FTC by calling 1-877-ID-THEFT (877-438-4338) or in writing at FTC Identity Theft Clearinghouse, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

9. **Report Any Misuse of your Personal Information:** If you have any reason to believe your information is being misused, contact law enforcement and file a police report. Provide a copy of the police report to your creditors to assist them in resolving any fraudulent activity. You can also contact the attorney general of your state and the Federal Trade Commission to report identity theft.

We deeply regret any inconvenience or concern that this breach of Premera's IT systems may cause you. If you have additional questions or concerns, please contact Premera at 1-800-768-5817 or Weyerhaeuser's Employee Service Center at 800-833-0030.

Sincerely,

Sharon Dusek

Sharon Dusek
Director, Compensation & Benefits