Abbott
Dept. D058E, Bldg. AP52
200 Abbott Park Road
Abbott Park, IL 60064

Tel: (877) 228-4707

March 13, 2015

Dear Active or Inactive Abbott Laboratories Health Care Plan Participant:

You may have or will soon receive a letter from Blue Cross Blue Shield of Illinois ("BCBSIL"). That letter will inform you that, as a result of the recent cyber-attack on Anthem Blue Cross Blue Shield ("Anthem"), certain personal information about you, your spouse and/or other dependents was possibly exposed. You will also receive (or may have already received) a similar letter from Anthem. It is very important that you review all communications that you receive from BCBSIL and/or Anthem, and then carefully follow the instructions laid out in them.

At this point, we have learned the following facts about this incident:

Anthem discovered on January 29, 2015 that it was the target of a cyber-attack that resulted in unauthorized access to its computer systems over the course of several weeks beginning in December 2014. The Abbott Laboratories Health Care Plan (the "Abbott Plan") is administered by BCBSIL and not by Anthem. However, Anthem plays a role in processing Abbott Plan claims for Abbott Plan participants who receive health care services in states where Anthem operates (California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia and Wisconsin). Consequently, personal information about some Abbott employees and other Abbott Plan participants who received care in those Anthem locations was exposed as a result of the incident. We are sending this notice to you because we have been advised by BCBSIL that it will be contacting you shortly by letter.

How are Abbott, BCBSIL and Anthem Responding to the Incident?

Abbott takes the protection of the privacy and security of your personal information very seriously. Since learning of the incident, we have been in regular contact with BCBSIL seeking to understand the extent to which Abbott Plan participant information may have been exposed. Anthem has stated that it immediately began a forensic investigation to determine what personal information may have been accessed and to identify affected individuals. It is our understanding that BCBSIL has confirmed the exact names of the affected individuals, and will be advising those persons via the letter noted above.

What Personal Information Was Involved in the Incident?

Though its investigation is still underway, Anthem states that initial results indicate that there was unauthorized access of current and former Abbott Plan participants, including names, dates of birth, member ID numbers, addresses, phone numbers, email addresses and/or employment information. We have no reason to believe credit/debit card or banking information was compromised, nor is there evidence at this time that medical information, such as claims, test results, or diagnosis/procedure codes, was obtained.

How Can I Learn Additional Information about the Incident?

We encourage you to visit Anthem's website dedicated to the incident – www.AnthemFacts.com (http://www.AnthemFacts.com) – where you can access Anthem's information about this incident. You may also call Anthem's dedicated toll-free number, 1-877-263-7995, to ask questions. In addition, Anthem and/or BCBSIL will be contacting you regarding this incident by mail. **You may also contact Abbott Human Resources at 877-228-4707 with any questions you may have.**

What Steps Can I Take to Protect Myself?

Regardless of whether unauthorized persons accessed your personal information as a result of this incident, any Abbott Plan participants who used their Blue Cross Blue Shield network in states where Anthem operates – California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia, and Wisconsin -- can enroll in free credit monitoring for a period of 24 months at http://www.AnthemFacts.com. Please note that the online enrollment process requires that you confirm you are or were enrolled in an Anthem or other Blue Cross Blue Shield plan at any point between 2004 to the present and to provide certain personal information.

In addition, provided below is information about additional steps you can take to prevent misuse of your personal information.

ADDITIONAL INFORMATION ABOUT IDENTITY THEFT PREVENTION

In addition to enrolling in the free credit monitoring service through the www.AnthemFacts.com website, we encourage you to consider the following other proactive steps designed to detect and prevent financial or medical identity theft or other misuse of your personal information:

Review Your Credit Reports

You should periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, P.O. Box105139, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion, P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

When you receive your credit reports, review them carefully for any sign of fraud such as accounts or creditor inquiries that you did not initiate or do not recognize, debts that you cannot explain, medical debt collection notices from health care providers or a home address or Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Review Your Account Statements and EOBs

- We recommend you remain vigilant with respect to reviewing your account statements, and promptly report any suspicious activity or suspected identity theft to Abbott and to the proper

law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission (FTC).

- Read the Explanations of Benefits (EOBs) that you receive from BCBSIL and other insurance companies. Make sure the health care claims to your insurers match the items and services that you received. Look for the name of the provider, the date of service and the service provided. If there is a discrepancy, contact BCBSIL or Abbott Human Resources immediately to report the problem.

Fraud Alerts

You should also consider placing a fraud alert to put your creditors and potential creditors on notice that you may be a victim of fraud. There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below:

Equifax: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Credit or "Security" Freezes

You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.*

Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified above (TransUnion, Experian and Equifax) to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

What if You Find Evidence of Identity Theft or Other Suspicious Activity?

We recommend that you promptly report any suspicious activity or suspected identity theft to the Abbott Plan and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the FTC. You may contact the FTC or your state regulatory authorities to obtain additional information about avoiding identity theft.

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

Warnings About Email and Phone Scams

Please be aware that scams have surfaced involving either emails that say they are from Anthem with attachments or web links (phishing) or fake telephone calls. You should be on high alert for such communications. Here are some critical scam/hoax email tips to bear in mind (specifically with respect to Anthem, although many of these may have broader applicability to email or phone scams generally):

- DO NOT click on any links in an email that look like they are coming from Anthem.
- DO NOT reply to any Anthem email or reach out to the senders in any way.
- DO NOT supply any information to any website that may open if you have clicked on a link in an Anthem-related email.
- DO NOT open any attachments that arrive with Anthem email.
- DO NOT provide any of your personal information over the phone if you receive a call from someone purporting to be from Anthem.
- DO check your credit card and bank statements for any suspicious charges or entries.
- DO check your credit reports periodically.

Again, **please ensure you review all communications that you receive from BCBSIL and/or Anthem, and then follow the instructions laid out in them.** As noted above, please feel free to contact Abbott Human Resources at **877-228-4707** if you have any questions relating to this letter.

Sincerely,
James L. Sipes
DVP Benefits & Wellness

79035194.4