Anthem®

To Members:

On January 29, 2015, Anthem, Inc. (Anthem) discovered that cyber attackers executed a sophisticated attack to gain unauthorized access to Anthem's IT system and obtained personal information relating to consumers who were or are currently covered by Anthem or other independent Blue Cross and Blue Shield plans that work with Anthem. Anthem believes that this suspicious activity may have occurred over the course of several weeks beginning in early December, 2014.

As soon as we discovered the attack, we immediately began working to close the security vulnerability and contacted the FBI. We have been fully cooperating with the FBI's investigation. Anthem has also retained Mandiant, one of the world's leading cybersecurity firms, to assist us in our investigation and to strengthen the security of our systems.

Consumers Impacted
Current or former members of one of Anthem's affiliated health plans may be impacted. In addition, some members of other independent Blue Cross and Blue Shield plans who received healthcare services through the BlueCard program in any of the areas that Anthem serves over the last 10 years may be impacted. The Blue Cross and Blue Shield Association's BlueCard program is a national program that enables members of one Blue Cross and Blue Shield Plan to obtain healthcare services while traveling or living in another Blue Cross and Blue Shield Plan's service area. Anthem is providing identity protection services to all individuals that are impacted. For a listing of potentially impacted Anthem affiliated health plans and other Blue Cross and Blue Shield companies for which Anthem provides services under the BlueCard program, visit AnthemFacts.com to view a list. You are receiving this message from Anthem as a current or former member of one of these potentially impacted companies.

Information Accessed
The information accessed may have included names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, employment information, including income data. We have no reason to believe credit card or banking information was compromised, nor is there evidence at this time that medical information such as claims, test results, or diagnostic codes, was targeted or obtained.

Identity Protection Services
Anthem has arranged to have AllClear ID protect your identity for two (2) years at no cost to you. The following identity protection services start on the date of this notice, or the date you previously enrolled in services based on information posted on AnthemFacts.com. You can use them at any time during the next two (2) years after your service begins.

- AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-263-7995 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear ID maintains an A+ rating at the Better Business Bureau.
- AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of fraud against children by searching thousands of databases for use of your child's information. To use the PRO service, you will need to provide your personal information to AllClear ID. To learn more about these services, or to enroll,

visit our source of truth www.AnthemFacts.com and click on the AllClear ID link from there. Please note: Additional steps may be required by you in order to activate your phone alerts.

Mailed Notification
Anthem will also individually notify potentially impacted current and former members by U.S. Postal mail with this same specific information on how to enroll in free credit monitoring and identity protection services. These services will be provided to potentially impacted current and former members free of charge. Anthem has also established a dedicated website (AnthemFacts.com) where members can access additional information, including frequently asked questions and answers.

Toll-Free Hotline
Anthem has established a dedicated toll-free number that you can call if you have questions related to this incident. That number is 877-263-7995. We have included contact information for the three nationwide credit bureaus below.

Si necesita información en español, ingrese en antheminforma.com.

Fraud Prevention Tips
We want to make you aware of steps you may take to guard against identity theft or fraud.

We recommend that potentially impacted members remain vigilant for incidents of fraud and identity theft, including by reviewing account statements and monitoring free credit reports. In addition, you can report suspected incidents of identity theft to local law enforcement, Federal Trade Commission, or your state attorney general. To learn more, you can go to the FTC's Web site, at www.consumer.gov/idtheft, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You should be aware of scam email campaigns targeting current and former Anthem members. These scams, designed to capture personal information (known as "phishing"), are designed to appear as if they are from Anthem and the emails include a "click here" link for credit monitoring. These emails are **NOT** from Anthem.

- DO NOT reply to the email or reach out to the senders in any way.
- DO NOT supply any information on the website that may open, if you have clicked on a link in email.
- DO NOT open any attachments that arrive with email.

Anthem is not calling members regarding the cyber-attack and is not asking for credit card information or Social Security numbers over the phone. For more guidance on recognizing scam email, please visit the FTC Website for their article on phishing.

Credit Bureau Information

Equifax	**Experian,**	**TransUnion**
PO BOX 740241	PO BOX 9532	PO BOX 6790
ATLANTA GA 30374-0241	ALLEN TX 75013	FULLERTON CA 92834-6790
1-800-685-1111	1-888-397-3742	1-800-916-8800
equifax.com	experian.com	transunion.com

You can obtain additional information from the FTC and the nationwide credit bureaus about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit bureaus listed above. As soon as that bureau processes your fraud

alert, it will notify the other two bureaus, which then must also place fraud alerts in your file. In addition, you can visit the credit bureau links below to determine if and how you may place a security freeze on your credit report to prohibit a credit bureau from releasing information from your credit report without your prior written authorization:

- Equifax security freeze: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
- Experian security freeze: http://www.experian.com/consumer/security_freeze.html
- TransUnion security freeze: http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

For Maryland and North Carolina Residents - You can obtain information from these sources about preventing identify theft:

- **Visit** the Federal Trade Commission website at: **www.ftc.gov, or call 1-877-ID-THEFT**
  or write to this address:
  Federal Trade Commission
  600 Pennsylvania Avenue NW
  Washington, DC 20580

- **Maryland:**
  Visit the Maryland Office of the Attorney General at:
  oag.state.md.us/idtheft/index.htm, or call 1-410-528-8662
  or write to this address:
  Consumer Protection Division
  Maryland Office of the Attorney General
  200 St. Paul Place
  Baltimore, MD 21202

- **North Carolina:**
  Visit the North Carolina Office of the Attorney General at: **http://www.ncdoj.gov/Crime.aspx** or call 1-919-716-6400 or write to this address:
  Attorney General's Office
  9001 Mail Service Center
  Raleigh, NC 27699-9001

FOR MASSACHUSSETTS RESIDENTS
Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies listed above.

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have

lived over the prior five years;
5. Proof of current address (e.g., a current utility bill or telephone bill);
6. A legible photocopy of a government issued identification card (e.g., state driver's license or ID card or military identification);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time To remove the security freeze, you must send a written request to each of the three credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.

Worried about links?
We know you might be concerned about clicking links, so Anthem did not include any in this message. However, some email programs and smart phones automatically add links. Remember, you can always type a web address manually in your browser instead of clicking through from this email.