

STATE OF NH
DEPT OF JUSTICE

2015 MAR -2 AM 11:59



February 20, 2015

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

Re: Notification of potential security breach

Dear Sirs/Madams:

Pursuant to New Hampshire state law, we are writing to inform you of an event which may constitute a breach of the security of personal information.

We have been notified by Anthem, Inc. that they have experienced a cyber-attack, potentially affecting as many as 80 million individuals. Anthem provides claims processing services for Highmark Blue Cross Blue Shield (BCBS), one of PNC's medical carriers, in certain states.

Highmark is an independent BCBS plan that partners with other BCBS plans to offer a national network of providers. When obtaining services in states where Highmark is not the local plan (outside Pennsylvania), a Highmark member or eligible family member's claims may be processed by the local BCBS plan, such as Anthem.

As a result, it has been determined that the personal information of some PNC employees (including former employees) and/or their eligible family members may have been compromised in the breach. While PNC's systems were not involved and not breached, we are submitting this notice as PNC is the owner of the data concerning the PNC employees and their family members affected.

Accessed information may have included names, dates of birth, Social Security Numbers, health care ID numbers, home addresses, email addresses and employment information, including income data. There is 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. Anthem is currently conducting an extensive IT forensic investigation to determine who is impacted.

All impacted individuals associated with PNC will receive notice via the U.S. Postal Service to their home address – either from Anthem or Highmark – within the next

The PNC Financial Services Group
One PNC Plaza 249 Fifth Avenue Pittsburgh Pennsylvania 15222-2707

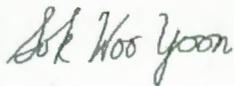
Confidential
www.pnc.com

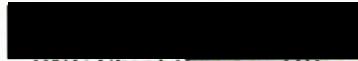
two weeks with details regarding protecting their identity and credit repair. Receipt of this letter is not confirmation that their information was compromised. A copy of the breach notification letter is attached for your reference.

PNC is continuing to work closely with Highmark and Anthem Blue Cross Blue Shield to better understand the cyber-attack and the impact on our employees. We will issue additional notices to your office as necessary as the situation continues to develop.

If you need any further information, please contact: 


Regards,




PNC Chief Privacy Officer

[Date of letter]

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. Anthem believes that this suspicious activity occurred over the course of several weeks beginning on December 10, 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.

Consumers Impacted

Current or former members of one of Anthem's affiliated health plans or other independent Blue Cross and Blue Shield plans may be impacted, and Anthem is providing identity protection services to you. For a listing of potentially impacted Anthem affiliated health plans and other Blue Cross and Blue Shield companies for which Anthem is providing this service, visit AnthemFacts.com to view a list. Anthem is a service provider to other group health plans and Blue Cross and Blue Shield plans across the country.

Information Accessed

The information accessed may have included names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses and 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 XXXX 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 to AnthemFacts.com. You can use them at any time during the next two (2) years after your service begins.

- XXXX: The team at XXX 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-XXX-XXX-XXXX 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. XXXX maintains an A+ rating at the Better Business Bureau.

- XXXX: 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, XXXX identifies acts of fraud against children by searching thousands of databases for use of your child's information. To use the XXXX service, you will need to provide your personal information to XXXX. To learn more about these services, or to enroll, visit our source of truth <http://www.AnthemFacts.com> and click on the XXXX 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 both current and former members can call if they have questions related to this incident. That number is: [XXX-XXX-XXXX]. We have included contact information for the three nationwide credit bureaus below.

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: <http://www.consumer.ftc.gov/articles/0003-phishing>.

Credit Bureau Information

Equifax

PO BOX 740241
ATLANTA GA 30374-0241
1-800-685-1111
equifax.com

Experian,

PO BOX 9532
ALLEN TX 75013
1-888-397-3742
experian.com

TransUnion

PO BOX 6790
FULLERTON CA 92834-6790
1-800-916-8800
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 1-919-716-6499
or write to this address: **Attorney General's Office**
9001 Mail Service Center