



0000001 01 SP 0.480 \*\*SNGLP T1 1 4444 00602-159797 \_ -C01-P00001-I

<NAME>  
<STREET ADDRESS>  
<CITY, ST ZIP>



Dear <NAME>:

On January 29, 2015, Anthem, Inc. (Anthem) learned of a cyberattack to our IT system. The cyberattackers tried to get private information about current and former Anthem members. We believe it happened over the course of several weeks beginning in early December 2014.

As soon as we learned about the attack, we:

- Began working to close the security issues
- Contacted the FBI to begin an investigation
- Hired Mandiant, a leading cybersecurity firm, to help with the investigation

We want to provide identity protection services to impacted members.

**Who is impacted?**

Current or former members of one of Anthem’s affiliated health plans may be impacted. These plans include but are not limited to **Amerigroup, UniCare, CareMore and HealthPlus Amerigroup**. You can visit [anthemfacts.com](http://anthemfacts.com) to view a list of Anthem plans that may be impacted. Anthem is a service provider to other group health plans and Blue Cross and Blue Shield plans across the country.

**What did the cyberattackers access?**

Accessed information may have included:

- Names
- Dates of birth
- Social Security numbers
- Health care ID numbers
- Home addresses
- Email addresses
- Work information like income data

We don’t believe these kinds of information were targeted or accessed:

- Credit card or banking information
- Medical information like claims, test results or diagnostic codes

**Cyberattack** – A crime that tries to damage, upset or take data from a computer, group or network when approval has not been given

**Cyberattackers** – People who try to damage, upset or take data from one computer, a computer group or network when approval has not been given

**Cybersecurity** – Steps taken to protect data from being damaged, upset or stolen from a computer, system or network

**Information technology (IT) system** – A computer group or network that handles data electronically

**Investigation** – To research what happened and who was part of a problem

## Identity Protection Services

We've arranged to have AllClear ID protect your identity for two years at no cost to you. These identity protection services start on the date of this notice. You can use them at any time during the next two years.

- AllClear Secure: The team at AllClear ID is ready and standing by if you need identity repair help. We're giving you this service at no cost. You don't need to enroll. If a problem comes up, just call 1-877-263-7995. An investigator will do the work to:
  - Recover financial losses
  - Restore your credit
  - Make sure your identity is returned to how it should be
- AllClear ID maintains an A+ rating at the Better Business Bureau.
- AllClear PRO: This service offers extra layers of protection, including:
  - Credit monitoring
  - A \$1 million identity theft insurance policy
  - For a child under 18 years old, AllClear ID ChildScan finds acts of fraud against children by searching data files for use of your child's information.
  - To use the PRO service, you'll need to provide your personal information to AllClear ID. To learn more about these services or to enroll:
    - Visit [anthemfacts.com](http://anthemfacts.com)
    - Click on the AllClear ID link from there

Please note: You may need to take extra steps to start your phone alerts.

## Mailed Notification

Anthem will tell all likely impacted current and former members by U.S. Postal Service how to enroll in free credit monitoring and identity protection services. These services will be given free of charge. Anthem has also set up a website ([www.anthemfacts.com](http://www.anthemfacts.com)) where you can learn more. Other members of your household may also get this letter if they were enrolled in an Anthem plan. Keep this letter in a safe place with your other important documents.

## Toll-Free Hotline

Anthem has set up a toll-free number for current and former members to call if they have questions about this incident. That number is 1-877-263-7995 or TTY/TDD 1-800-855-2880. Contact information for the three nationwide credit bureaus is given on the next page.

## Fraud Prevention Tips

There are steps you may take to guard yourself against identity theft or fraud.

**Identity protection services** – A company that helps keep personal data private and safe

**Identity** – Anything that makes someone different from everyone else

**Credit monitoring** – A service or company that watches your credit card accounts for strange events or charge

**Personal and private information** – Any data about a living person, for example: name, birthdate, Social Security number or address

**Credit bureau** – A company which saves data about the way someone uses credit, and assigns a credit score

**Fraud** – The crime of using dishonest steps to take something from someone else to cause harm



We urge likely impacted members to stay alert for incidents of fraud and identity theft. This includes reviewing your account statements and checking free credit reports. Also, you can report suspected incidents of identity theft to local law enforcement, the Federal Trade Commission (FTC) or your state attorney general. To learn more, you can:

- Go to the FTC website at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)
- Call the FTC at 1-877-IDTHEFT (1-877-438-4338) or
- Write to:  
Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue NW  
Washington, DC 20580

**Identity theft** – When personal data has been taken by someone who wants to harm

**Credit report** – A report with information on a person’s credit history including credit accounts, loans and late payments.

You should be aware of scam email campaigns that target current and former Anthem members. These scams are called “phishing.” They’re meant to look like they’re from Anthem. These 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 enter 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 about the cyberattack. Also, Anthem is not asking for credit card information or Social Security numbers over the phone. For more help on spotting scam email, please visit the FTC website at [www.consumer.ftc.gov/articles/0003-phishing](http://www.consumer.ftc.gov/articles/0003-phishing).

Credit Bureau Information

<p><b>Equifax</b> PO BOX 740241 ATLANTA GA 30374-0241 1-800-685-1111 <a href="http://equifax.com">equifax.com</a></p>	<p><b>Experian</b> PO BOX 9532 ALLEN TX 75013 1-888-397-3742 <a href="http://experian.com">experian.com</a></p>	<p><b>TransUnion</b> PO BOX 2000 CHESTER PA 19022 1-800-916-8800 <a href="http://transunion.com">transunion.com</a></p>
---	---	---

You can get more information from the FTC and the 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 harder for someone to get credit in your name. This is because it tells creditors to follow certain steps to protect you, but it also may slow your ability to get credit.

**Fraud alert** – An alert put on a credit card account when an event or charge does not show how the account owner most often acts

You may place a fraud alert in your file by calling one of the credit bureaus listed above. When that bureau helps to process your fraud alert, it will tell the other two bureaus. They will then also place fraud alerts in your file.

Also, you can visit the credit bureau links below to find out if and how you may place a security freeze on your credit report. This can stop a credit bureau from sharing information from your credit report without your prior written consent:

**Security freeze** – A notice put in a person’s credit report. It helps protect them from being a victim of identity theft.

- Equifax security freeze: [https://www.freeze.equifax.com/Freeze/jsp/SFF\\_PersonalIDInfo.jsp](https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp)
- Experian security freeze: [www.experian.com/consumer/security\\_freeze.html](http://www.experian.com/consumer/security_freeze.html)
- TransUnion security freeze: [www.transunion.com/personal-credit/credit-disputes/credit-freezes.page](http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page)

For Maryland and North Carolina residents — you can get information from these sources about helping to prevent identify theft:

**Federal Trade Commission**

- Visit the FTC website at [www.ftc.gov](http://www.ftc.gov)
- Call 1-877-ID-THEFT or
- Write to:  
Federal Trade Commission  
600 Pennsylvania Avenue NW  
Washington, DC 20580

**Maryland**

- Visit the Maryland Office of the Attorney General website at [www.oag.state.md.us/idtheft/index.htm](http://www.oag.state.md.us/idtheft/index.htm)
- Call 1-410-528-8662 or
- Write to:  
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 website at [www.ncdoj.gov/Crime.aspx](http://www.ncdoj.gov/Crime.aspx)
- Call 1-919-716-6400 or
- Write to:  
Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001

Si necesita esta correspondencia en español, llame al 1-877-263-7995 o TTY/TDD 1-800-855-2884.