

IMPORTANT INFORMATION ABOUT THE ANTHEM CYBER ATTACK BREACH

Dear Employees:

We know that many of you are probably concerned about the ramifications of the Anthem breach last week, as are we. It is important that you are aware of the situation and protect yourselves as best you can from this and other breaches.

Here is what we know about the Anthem breach.

- Anthem was the target of a very sophisticated external cyber attack.
- These cyber attackers gained unauthorized access to Anthem's Information Technology (IT) system and have obtained personal information from its current and former members, such as their names, birthdays, member health ID numbers/Social Security numbers, street addresses, email addresses and employment information, including income data.
- Anthem's investigation to date indicates there is no evidence that banking, financial or medical information, such as claims, test results, or diagnostic codes were targeted or compromised.
- Once the attack was discovered, Anthem immediately made every effort to close the security vulnerability, contacted the Federal Bureau of Investigation (FBI) and began fully cooperating with their investigation. Anthem has also retained Mandiant, one of the world's leading cybersecurity firms, to provide incident response and security assessment services.
- Anthem is not aware of any fraud that has occurred as a result of this incident against its members, but all impacted members will be enrolled in identity repair services. In addition, impacted members will be provided information on how to enroll in free credit monitoring.
- Anthem has created a dedicated website (www.AnthemFacts.com) where you and other members can access information such as frequent questions and answers and a phone number that members can call 1-877-263-7995.

Frequently Asked Questions:

Was my information accessed?

Anthem is currently conducting an extensive IT forensic investigation to determine what members are impacted. The Anthem teams are working around the clock to determine how many people have been impacted and will notify all Anthem members who are impacted through a written communication.

What information was compromised?

Anthem's initial investigation indicates that the member data accessed included names, dates of birth, member health ID numbers/Social Security numbers, addresses, phone numbers, email addresses and employment information including income data.

Was there any diagnosis or treatment data exposed?

Anthem's investigation to date indicates there is no evidence that medical information, such as claims, test results, or diagnostic codes were targeted or compromised.

Was my credit card information accessed?

Anthem's investigation to date indicates there is no evidence that credit card information was compromised.

Do the people who accessed my information have my Social Security number?

Anthem's investigation to date indicates that the information accessed included names, dates of birth, member health ID numbers/Social Security numbers, street addresses, email addresses and employment information. Anthem is working to determine whose Social Security numbers were accessed.

How can I sign up for credit monitoring services?

All impacted members will receive notice via mail which will advise them of the protections being offered to them as well as any next steps.

When will I receive my letter in the mail?

Anthem will continue working to identify the members who are impacted. We expect the mailing of letters to begin in the next two weeks.

My children are on my insurance plan, was their information also accessed?

Anthem is currently conducting an extensive IT forensic investigation to determine which members are impacted; however, adults and children were impacted.

Do the people who accessed my information know about my medical history?

Our investigation to date indicates there was no diagnosis or treatment data exposed.

Do the people who accessed my information have my credit card numbers and banking information?

No, the investigation to date indicates that information accessed did not include credit card numbers, banking or other financial information.

Has anyone used my information yet?

We are not aware of any fraud that has occurred as a result of this incident against our members

Am I at risk for identity theft?

Anthem is currently conducting an extensive IT forensic investigation to determine which members are impacted. We are not aware of any fraud that has occurred as a result of this incident against our members, but all impacted members will be enrolled in identity repair services. In addition, impacted members will be provided information on how to enroll in free credit monitoring.

Do I need a new member ID card and number?

Anthem is working around the clock to determine how many people have been impacted and will notify all who are impacted. Anthem will provide further guidance on next steps.

How can I be sure my personal and health information is safe with Anthem, Inc.?

Safeguarding its members' personal, financial and medical information is a top priority for Anthem, and because of that, they have a state-of-the-art information security system to protect the data.

Anthem has contracted with Mandiant – a global company specializing in the investigation and resolution of cyber attacks. Anthem will work with Mandiant to ensure there are no further vulnerabilities and work to strengthen security.

What is Anthem doing to help members potentially affected by this incident?

All impacted members will be enrolled in identity repair services. In addition, impacted members will be provided information on how to enroll in free credit monitoring.

Where is the data now? And who can access my information?

Evidence indicates that the data was uploaded to an external file sharing service. This file sharing service, at Anthem's request, has locked down the account and data so that it cannot be copied, accessed or removed. Anthem and the FBI are working with the file sharing service to access the data and further secure it.

Beware of Phishing Email Scams

Since this initial information was released, we have heard that email scams (known as “phishing”) have begun. The following information is to assist you in avoiding further damage. Members who may have been impacted by the cyber attack against Anthem should be aware of scam email campaigns targeting current and former 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.** If you or one of your family members should receive these emails:

- DO NOT click on any links in email.
- 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 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 are not asking for credit card information or social security numbers over the phone.

This outreach is from scam artists who are trying to trick consumers into sharing personal data. There is no indication that the scam email campaigns are being conducted by those that committed the cyber attack, or that the information accessed in the attack is being used by the scammers.

Anthem will contact current and former members via mail delivered by the U.S. Postal Service about the cyber attack with specific information on how to enroll in credit monitoring. Affected members will receive free credit monitoring and ID protection services.

For more guidance on recognizing scam email, please visit the FTC Website:
<http://www.consumer.ftc.gov/articles/0003-phishing>.

Anthem has created a dedicated website (www.AnthemFacts.com) where everyone can access information such as frequently asked questions and answers.

We strongly urge you to sign up for the credit monitoring/repair services offered by Anthem once you receive the information in the mail.

Sincerely,

[Insert Employer Name]