Producer Bulletin

Capital BLUE

Anthem Data Breach

Producer Communication #700
Issued February 9, 2015
Updated February 13, 2015

Message

Anthem, Inc., the nation's second-largest health insurance company, has reported that it was the target of a sophisticated external cyber attack. This attack resulted in unauthorized access to the personal information of up to 80 million members. Anthem offers Blue plans in California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia, and Wisconsin.

Details

Capital BlueCross is working closely with Anthem and the Blue Cross Blue Shield Association to specifically determine if the information of any of our current or former members was included in this cyber attack. Notification will be provided to impacted members and groups in the coming weeks. Talking points have been developed by our IT, Privacy Office and Communications teams related to this issue and its impact on Capital BlueCross (Attachment A). Producers may reference these talking points when assisting their customers with inquiries however these should not be shared directly with the group.

Since learning of the Anthem cyber-attack, Capital BlueCross has been working diligently to gather more information about the breach and how it might impact any of our members.

Anthem continues to work with federal and state authorities to investigate the breach. The investigation is ongoing and no responsible party has been reported to date.
Anthem's investigation to date indicates there is no evidence that credit card or medical information was targeted or compromised.

Capital BlueCross systems were not impacted by, and were not a part of, the Anthem breach. However, some of our members who received health care services in any of the areas that Anthem serves during the last 10 years may have been affected by the Anthem breach. (*Anthem offers Blue plans in California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia, and Wisconsin.)*

It is our understanding that any CBC member who did not receive health care services in geographic areas covered by Anthem was not impacted by this breach.

Anthem has provided Capital BlueCross with data to determine if any of our members are impacted and we are reviewing that information now. This process will take some time but, once completed, we will be working with Anthem to ensure that affected members are notified and that proper assistance is offered.

Anthem will handle the notifications to non-Anthem affected members. Once Anthem's notification mailings are set to begin, CBC will notify ASO and insured group administrator contacts so they are provided with advance notice that their employees will be receiving notification from Anthem.

Additionally, Anthem has announced that it is providing two years of free identity protection services for all current and former BlueCross BlueShield members whose information was affected. The services include: credit monitoring, fraud detection, identity repair, and identity theft insurance. Members can learn how to enroll for these services at AnthemFacts.com prior to receiving mailed notification from Anthem, which will be sent in the coming weeks.

Identity Protection Services Details:
All current and former Blue Cross Blue Shield members whose information was impacted by the Anthem cyber-attack can enroll in these services beginning Friday, February 13. This includes Anthem and non-Anthem Blue members. The free identity protection services provided by Anthem include two years of:

- *Identity Repair Assistance:* Should a member experience fraud, an investigator will do the work to recover financial losses, restore the member's credit, and ensure the member's identity is returned to its proper condition. This assistance will cover any fraud that has occurred since the incident first began.

- *Credit Monitoring:* At no cost, members may also enroll in additional protections, including credit monitoring. Credit monitoring alerts consumers when banks and creditors use their identity to open new credit accounts.

- *Child Identity Protection:* Child-specific identity protection services will also be offered to any members with children insured through their Anthem plan.

- *Identity theft insurance:* For individuals who enroll, the company has arranged for $1,000,000 in identity theft insurance, where allowed by law.

- *Identity theft monitoring/fraud detection:* For members who enroll, data such as credit card numbers, social security numbers and emails will be scanned against aggregated data sources maintained by top security researchers that contain stolen and compromised individual data, in order to look for any indication that the members' data has been compromised.

- *Phone Alerts:* Individuals who register for this service and provide their contact information will receive an alert when there is a notification from a credit bureau, or when it appears from identity theft monitoring activities that the individual's identity may be compromised.

Below is our media statement (updated as of February 13, 2015) that will be used if we receive any inquiries, as well as what is now posted to our Capital BlueCross website:

> *Capital BlueCross is diligently working to gather more information about the Anthem Inc. cyber-attack and how it might impact any of our members.*

Capital BlueCross systems were not impacted by, and were not part of, the Anthem breach. Capital BlueCross and Anthem are separate and distinct companies.

However, some of our members who received health care services in any of the areas that Anthem serves during the last 10 years may have been affected by the Anthem breach. This is because 37 independent, locally operated companies across the United States form the BlueCross BlueShield system. This affiliation enables BlueCross BlueShield customers to get the high-quality, affordable health care they need wherever they are.

Areas served by Anthem include: California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia and Wisconsin.

Anthem has announced that starting on February 13, 2015, it is providing 24 months of free identity protection services for all current and former BlueCross and BlueShield members dating back to 2004 who feel their information was affected. The services include: credit monitoring, fraud detection, identity repair, and identity theft insurance. Members can learn how to enroll for these services at AnthemFacts.com. Members may access these services at any time during the 24-month coverage period.

For additional information and resources about the Anthem situation, please visit www.AnthemFacts.com or call their dedicated toll-free hotline at 1-877-263-7995.

Anthem issued a set of talking points (Attachment B) and established a website to provide information about this data breach. Keep in mind that this information is specific to Anthem customers.

Attachments

- **Attachment A –** Talking points developed by our IT, Privacy Office and Communications teams
- **Attachment B –** Talking points developed by Anthem

Questions

Contact your Preferred Agency with any questions. Thank you.

Confidential
Not for direct customer distribution

Anthem Data Breach Talking Points and Q&As-February 13, 2015
Developed by Capital BlueCross IT, Privacy Office and Communications teams

- Anthem and its affiliated brands were the target of a very sophisticated external cyber attack.

- The cyber attackers gained unauthorized access to Anthem's information technology (IT) system and obtained personal information from current and former members such as names, birthdays, member identification (ID) and/or Social Security numbers, street addresses, email addresses and employment information, including income data. This system contained files dating back to 2004.

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

- Capital BlueCross systems were not impacted by, and were not a part of, the Anthem breach.

- There is the potential that a Capital BlueCross member's information could be involved in this breach if the member received health care services in the geographic areas covered by Anthem. (*Anthem offers Blue plans in California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia, and Wisconsin.)*

- It is our understanding that any CBC member who did not receive health care services in geographic areas covered by Anthem was not impacted by this breach.

- Anthem has provided Capital BlueCross with data to determine if any of our members are impacted and we are reviewing that information now. This process will take some time but, once completed, we will be working with Anthem to ensure that affected members are notified and that proper assistance, including free credit monitoring and identity protection services, is offered.

- Anthem has established a website to provide information about this data breach: www.anthemfacts.com. The website is being updated as Anthem's investigation progresses. Beginning Friday, February 13, 2015, this site will provide information on how affected members can enroll in credit monitoring and identity protection services, even if the member has not yet received notification from Anthem.

- Safeguarding your personal information is of the utmost importance to Capital BlueCross.

- The following administrative and technical safeguards are in place to protect your information:

    - Dedicated and knowledgeable IT security personnel proactively manage data security day-to-day including vulnerability analysis, security risk assessments, and incident response
    - Technologies are in place to safeguard IT systems and equipment accessed and used by employees, members, providers, and business partners
    - Third-party information security organizations and subject matter resources are contracted to provide continuous monitoring of our IT systems. Third-parties also perform periodic IT security reviews to assess the state of our data security program and compliance with state and federal regulatory requirements

Confidential
Not for direct customer distribution

Questions & Answers

Q: Has Anthem provided Capital BlueCross with information about Capital BlueCross members impacted by the cyber attack?

A: Anthem has provided Capital BlueCross with information to determine if any Capital BlueCross members are impacted by the cyber-attack on Anthem and the data disclosure that resulted from the attack. We are reviewing that information now. Once that process is completed, we will be working with Anthem to ensure proper notification to affected members takes place and proper assistance is offered.

Q : How many Capital BlueCross members were impacted?

A: We are reviewing the information now.

Q: When will Capital BlueCross members know if they were impacted?

A: Anthem will notify members if they are impacted by the cyber attack. Anthem will provide credit monitoring and identity protection services free of charge so that those who have been affected can have peace of mind. Details about these services will be included in a direct notice to anyone affected and information will be available on the Anthem website, AnthemFacts.com

Q: I am not a member of an Anthem Plan. Why was my personal information impacted?

A: Some of our members who received healthcare services in any of the areas that Anthem serves during the last 10 years may have been affected by this breach. That's because 37 independent, locally operated companies across the U.S. form the BlueCross BlueShield system. This affiliation enables BlueCross BlueShield customers to get the high-quality, affordable healthcare they need wherever they are.

Q: How can I sign up for credit monitoring/identity protection services?

A: Anthem has announced that starting on February 13, 2015, it is providing 24 months of free identity protection services for all current and former BlueCross and BlueShield members dating back to 2004 who feel their information was affected. The services include: credit monitoring, fraud detection, identity repair, and identity theft insurance. Members can learn how to enroll for these services at AnthemFacts.com. Members may access these services at any time during the 24-month coverage period.

Q: What credit monitoring/identity protection services will be made available to those affected by the Anthem cyber-attack?

A: All current and former Blue Cross Blue Shield members whose information was impacted by the Anthem cyber-attack can enroll in these services beginning Friday, February 13. This includes Anthem and non-Anthem Blue members. The free identity protection services provided by Anthem include two years of:

- *Identity Repair Assistance:* Should a member experience fraud, an investigator will do the work to recover financial losses, restore the member's credit, and ensure the member's identity is returned to its proper condition. This assistance will cover any fraud that has occurred since the incident first began.
- *Credit Monitoring:* At no cost, members may also enroll in additional protections, including credit monitoring. Credit monitoring alerts consumers when banks and creditors use their identity to open new credit accounts.

- *Child Identity Protection:* Child-specific identity protection services will also be offered to any members with children insured through their Anthem plan.

- *Identity theft insurance:* For individuals who enroll, the company has arranged for $1,000,000 in identity theft insurance, where allowed by law.

- *Identity theft monitoring/fraud detection:* For members who enroll, data such as credit card numbers, social security numbers and emails will be scanned against aggregated data sources maintained by top security researchers that contain stolen and compromised individual data, in order to look for any indication that the members' data has been compromised.

- *Phone Alerts:* Individuals who register for this service and provide their contact information will receive an alert when there is a notification from a credit bureau, or when it appears from identity theft monitoring activities that the individual's identity may be compromised.

Confidential
Not for direct customer distribution

Anthem Data Breach Q&A. Please note that this is the information that Anthem has at this time.

- Anthem and its affiliated brands were 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 our current and former members such as their names, birthdays, member identification (ID) and/or Social Security numbers, street addresses, email addresses and employment information, including income data.
- Our investigation to date indicates there is no evidence that credit card or medical information was targeted or compromised. Provider information was not compromised.
- We will begin to mail letters to impacted members in the coming weeks, if your information has been accessed, we will provide free identity repair services and credit monitoring so that you can have peace of mind.
- Your security is very important to us. We are very sorry for what has happened and the inconvenience it has caused. We will continue to do everything in our power to make our systems more secure.
- We have created a website (www.AnthemFacts.com) where you can learn more. This website will continue to be updated as the investigation progresses.

Member FAQ

1. **Was my information accessed?**
   Anthem is currently conducting an extensive IT forensic investigation to determine what members are impacted. We 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.

2. **When will I receive my letter in the mail?**
   We continue working to identify the members who are impacted. We will begin to mail letters to impacted members in the coming weeks.

3. **How can I sign up for credit monitoring/identity protection 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.

4. **When did Anthem find out?**
   On January 29, 2015, we determined that we were the victim of a sophisticated cyber attack. We immediately notified federal law enforcement officials.

5. **Does my employer know about this incident?**
   We are in the process of notifying employers of this cyber breach.

6. **Who is responsible for this cyber attack or breach?**
   Anthem is working closely with federal law enforcement investigators. At this time, no one person or entity has been identified as the attacker.

7. **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.

8. **Do the people who accessed my information know about my medical history?**
   No - our investigation to date indicates there was no diagnosis or treatment data exposed.

9. **Do the people who accessed my information have my credit card numbers?**
   No, our current investigation shows the information accessed did not include credit card numbers.

10. **Do the people who accessed my information have my Social Security number?**
    Our investigation to date indicates that the information accessed included names, dates of birth, member ID and/or Social Security numbers, street addresses, email addresses and employment information. We are working to determine whose Social Security numbers were accessed.

11. **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.

12. **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 eligible to receive identity repair assistance. Identity repair services provide affected customers with a dedicated investigator to assist them with fraud-related issues arising from this incident. In addition, impacted members will be provided information on how to enroll in free credit monitoring.

13. **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. Your current member ID card and number are valid and will provide you access to care.

14. **Will this make my insurance premiums go up?**
    No. This should not have an impact on your insurance premiums.

15. **What information has been compromised?**
    Initial investigation indicates that the member data accessed included names, member ID numbers, dates of birth, Social Security numbers, addresses, telephone numbers, email addresses and employment information.

16. **Was provider data accessed?**
    Our investigation to date indicates that no provider data was accessed.

17. **Was there any diagnosis or treatment data exposed?**
    No, we do not believe any diagnosis or treatment data was exposed.

18. **Does this incident affect members as well as anyone who has applied for insurance during open enrollment on the health insurance marketplace?**
    At this time, we are conducting a thorough IT forensic investigation to determine whose information was accessed.

19. **What measures have you taken to protect against further hacking or breaches?**
    Anthem Information Security has worked to eliminate any further vulnerability and continues to secure all its data. Cyber attacks are continually evolving and cyber attackers are becoming more sophisticated every day. We are also working with federal law enforcement on this investigation and to ensure our environment is as secure as possible.

20. **How can I be sure my personal and health information is safe with Anthem, Inc.?**
    Anthem is doing everything it can to ensure there is no further vulnerability to its database warehouses. Anthem has contracted with a global company specializing in the investigation and resolution of cyber attacks. We will work with this company to reduce the risk of any further vulnerabilities and work to strengthen security.

21. **What are you doing to help members potentially affected by this incident?**
    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.

22. **Did this impact all lines of Anthem Business?**
    Yes, all product lines are impacted.

23. **Does this impact all of Anthem's Affiliated Health Plans?**
    Yes, impacted brands include Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, CareMore, UniCare, HealthLink, and DeCare.

24. **Are only current members impacted?**
    Our investigation to date shows this incident affects members whose data was contained in the database warehouse. Current and some prior members, including minors and adults in all 50 states and some international residents, may be impacted.

25. **Is my (plan/brand) impacted?**
    The impacted (plan/brand) include Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, CareMore, UniCare, HealthLink, and DeCare.

26. **I'm not an Anthem member; I am a member of a non-Anthem Blue Cross Blue Shield Plan. Was my information accessed?**

Anthem is currently conducting an extensive IT forensic investigation to determine what members are impacted. We are working around the clock to determine how many people have been impacted and will notify you if you are impacted through a written communication. Some members of other Blue Cross Blue Shield plans may be impacted. We are working with other Blue plans to ensure communications are delivered to their members.

27. **Would I be able to file a grievance related to this cyber attack?**
    Although a grievance filing would not be applicable for a cyber attack, we are very sorry for what has happened and the inconvenience it has caused. We will begin to mail letters to impacted members in the coming weeks, if your information has been accessed, we will provide free identity repair services and credit monitoring so that you can have peace of mind.

28. **I live in California, would I be able to file a one day grievance related to this cyber attack?**
    Although a grievance filing would not be applicable for a cyber attack, we are very sorry for what has happened and the inconvenience it has caused. We will begin to mail letters to impacted members in the coming weeks, if your information has been accessed, we will provide free identity repair services and credit monitoring so that you can have peace of mind.