Producer Bulletin

Capital BLUE

Anthem Data Breach

Producer Communication #700
Issued February 9, 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.

Though Capital BlueCross systems were not impacted by and were not a part of the Anthem breach, it is important to understand 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. It is our understanding that any CBC member who did not receive health care services in these areas would not be impacted by this breach.

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.

Additionally, below is our media statement that will be used if we receive any inquiries, as well as what is now posted to our Capital BlueCross website:

> *Capital BlueCross is aware of the Anthem Inc. cyber-attack and we are diligently working to gather more information and understand the scope of this issue and how it might impact any of our members.*
>
> *The Blue Cross and Blue Shield System consists of 37 independently operated Blue Cross and Blue Shield member companies. Capital BlueCross and Anthem Inc. are separate and distinct companies, though through various collaborative agreements some information on Capital BlueCross members could have been affected.*
>
> *We are working in collaboration with all BCBS Plans to ensure that the most state-of-the-art information security systems are in place to protect each of our members. For additional information and resources about the Anthem situation, including assistance Anthem is providing to customers, 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

Developed by Capital BlueCross IT, Privacy Office and Communications teams

- 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.

- 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. It is our understanding that any CBC member who did not receive health care services in these areas would not be impacted by this breach.

- For members impacted by the breach, there is the potential that some or all of the following information may have been accessed: name, SSN, member ID number, date of birth, address, phone number, email address, and employment information, including income. Anthem believes that no claim information and no credit card information were accessed.

- 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.

- Anthem has established a website to provide information about this data breach: http://www.anthemfacts.com

- Initial investigation indicates that this attack was targeted specifically at Anthem and not Capital BlueCross or the BlueCross BlueShield Association as a whole. Capital BlueCross has no indication that it is being specifically targeted in a similar manner, nor were its IT systems part of the cyber attack reported by Anthem, Inc.

- Safeguarding your personal information is of the utmost importance to Capital BlueCross. We have implemented the following administrative and technical safeguards to protect your information:
  - We have dedicated and knowledgeable IT security personnel responsible for day-to-day information security matters, including incident response, vulnerability analysis, and security risk assessments;
  - Technologies have been implemented to provide technical safeguards for the IT systems and equipment used and accessed by our employees, members, providers and business partners;
  - Third-party information security organizations and subject matter resources are contracted with to provide continuous monitoring of our IT systems. Third-parties also perform periodic IT security reviews to assess the state of our security program and how it aligns to our state and federal regulatory requirements

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.