Producer Bulletin

Capital BLUE

Excellus BlueCross Blue Shield Cyber-Attack

Producer Communication #732
Issued September 18, 2015
Updated October 5, 2015

Message

On September 9, 2015, Excellus BlueCross BlueShield announced that their information technology systems were the target of a sophisticated cyber-attack.

Capital BlueCross systems were not impacted by, and were not part of, the attack on Excellus' systems. Capital BlueCross and Excellus are separate and distinct companies.

However, because the attack involved BlueCard data on Excellus' IT system, members of other Blue Plans, including Capital BlueCross, may be affected if they have received services in the Excellus service area.

Details

Excellus BlueCross BlueShield, headquartered in Rochester, New York covering 31 counties in upstate New York, announced that the company was the victim of a cyber-attack during which attackers gained unauthorized access to Excellus' information technology system. The attack was discovered on August 5, 2015 and the subsequent investigation revealed that the initial attack occurred on December 23, 2013 and involves information that dates back to 1980. It is our understanding, however, that any data accessed about BlueCard members, which would include any affected CBC members, dates back to 1993.

Since learning of the Excellus cyber-attack, Capital BlueCross has been working diligently to gather information about the attack on Excellus and how it might impact any of our members. The Excellus attack involved the information of members of other BlueCross and BlueShield plans who sought treatment in Excellus' service area. That is because 36 independent, locally operated companies across the U.S. form the BlueCross BlueShield system. This affiliation enables BlueCross and BlueShield customers to get the high-quality, affordable health care they need wherever they are. If a member has not received health care services in Excellus' service area in central New York since 1993, their information should not be at risk.

As part of its investigation, Excellus notified the FBI and is coordinating with the Bureau's investigation into this attack. Excellus also worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct a comprehensive investigation of the incident and to remove the infection created by the attack. Excellus is also taking additional steps to strengthen and enhance the security of their system.

According to Excellus, attackers may have gained unauthorized access to members' information, which for any of our affected members, could include name, date of birth, address, telephone number, Social Security number, member identification number, financial account information, and claims information. More information about this incident can be found at www.excellusfacts.com.

Letters will be mailed from Excellus to all affected individuals and they will be provided with two years of free credit monitoring and identity theft protection services from Kroll, a global leader in risk mitigation and response, with an additional two years of free identity restitution services for incidents identified during the initial two-year period. Individuals who believe they may have been affected by this attack and want to enroll in these services before receiving their letter, may do so by following the instructions for enrollment found at: www.excellusfacts.com or by calling the dedicated hotline at 877.589.3331.

Excellus delayed announcing the cyber-attack until they closed the vulnerability on their system, and could more clearly determine the individuals that are potentially affected.

At this time, Excellus has no evidence that any data was removed at any point during this attack. They also have no evidence such data has been used inappropriately since the attack.

Notification to Affected Members and ASO Group Customers
Last week, Excellus began sending notifications by U.S. mail to impacted Excellus members.

Excellus will send letters to affected BlueCard members, including affected Capital BlueCross members, only after completion of a member verification process by each Plan. Capital BlueCross is working with Excellus to identify any impacted Capital BlueCross members. Once identified, we will work to alert our current and former ASO groups as we have done in the past in advance of the Excellus mailing to the affected members. More details will be provided as they become available.

On or about October 12, Excellus plans to begin sending notifications by U.S. mail to BlueCard members, including Capital BlueCross members, whose information may have been accessed. There are two versions of these notifications: one for impacted adults and one for impacted children under the age of 18 at the time of the mailing. Mailings to affected members may take several weeks.

On or about October 5, Capital BlueCross will send letters to ASO group customers (active and former) that have affected members to provide advance notice that their affected members will receive notification from Excellus by U.S. mail.

Active ASO groups will be directed to contact their Capital BlueCross Account Executive or producer with questions. A copy of the letter to active ASO groups is attached (*Attachment C*). A list of the group's current and/or former members affected by the Excellus breach will be included with this letter. The list will also indicate whether each member's Social Security number may have been involved. A copy of Excellus' member notification letters to adults and minors will also be included as enclosures and are attached to this bulletin (*Attachments E and F*).

Former ASO groups will be notified via their letter that a list of the names of their group's affected current and/or former members can be requested by sending a letter requesting this information, on their company letterhead, to Capital BlueCross' Privacy Office. The letter directs former ASO groups with questions to call the Group Services line at 866.814.7544. A team of Customer Service representatives is prepared specifically to address calls generated by the letter to former ASO groups. A copy of the letter to former ASO groups is attached (*Attachment D*) and the copy of Excellus' member notification letters will be included as enclosures (*Attachments E and F*).

- If another BlueCross BlueShield system plan served as the affected group customer's administrator since 1993, groups may receive a letter from that plan in addition to the letter we are sending; however, affected members will only receive one notification from Excellus.

- ASO groups may have members who receive an Excellus notification who are not included on the member list enclosed with their Capital BlueCross group letter. This may be because those individuals were enrolled in a plan sometime since 1993 that was administered by another BlueCross BlueShield system plan, such as one that may have been offered through a different employer.

As with other recent cyber-attacks, a business decision has been made to not send letters to fully insured groups.

Producer Bulletin

Capital BLUE

HITECH Breach Notification and the U.S. Department of Health and Human Services
Excellus has provided preliminary notification to the U.S. Department of Health and Human Services (HHS) about the attack on its systems, and will be providing subsequent notification to the Department with all of the required information. Excellus' notification to HHS will cover all affected BlueCross BlueShield system self-funded group health plans, so there is no need for our ASO group customers to make a separate notification to HHS.

Capital BlueCross' Commitment to Information Security
Protecting member information is of the utmost importance to Capital BlueCross and we maintain a vigilant data security program.

From state-of-the-art technology, to continuous monitoring of our systems, we work to ensure that the best technical and administrative safeguards are in place. Additionally, we contract with third-party information security organizations and subject matter resources to provide continuous monitoring of our systems.

In light of recent attacks on other companies in the health insurance industry, Capital BlueCross also has undertaken additional actions to strengthen the company's information technology systems and data security program.

Talking Points and Capital BlueCross' External Statement
Attached for your convenience are talking points and Q&As (*Attachment A*) as well as Capital BlueCross' external statement posted on capbluecross.com (*Attachment B*).

Attachments

- **Attachment A –** Excellus Talking Points/Q&A
- **Attachment B –** CBC's external statement: Excellus Cyber-Attack
- **Attachment C –** Letter to impacted active ASO groups
- **Attachment D –** Letter to impacted former ASO groups
- **Attachment E –** Excellus letter to impacted adult members
- **Attachment F –** Excellus letter to impacted minor members

Questions

Contact your Preferred Agency with any questions. Thank you.