

EXCELLUS BLUE CROSS BLUE SHIELD TALKING POINTS and Q&As

Talking Points

- On August 5, 2015, Excellus discovered that cyber attackers executed a sophisticated attack to gain unauthorized access to Excellus' information technology system.
- More information about the Excellus cyber-attack may be found at www.excellusfacts.com.
- Excellus discovered signs of the cyber-attack in collaboration with Mandiant, one of the world's leading cybersecurity firms.
- Excellus' investigation revealed that the initial attack occurred on December 23, 2013.
- The information involved in the Excellus incident, in some cases, dates back to 1980 and impacts nearly 10,000 million individuals.
- The Excellus attack involved the information of some members of other BlueCross and BlueShield plans, including Capital BlueCross, who sought treatment in Excellus' service area, since 1993. Excellus is headquartered in Rochester, New York and covers [31 counties in upstate New York](#).
- These members were affected because Capital BlueCross is one of 37 independent, locally operated companies across the United States that form the BlueCross BlueShield system. This affiliation enables BlueCross and BlueShield plan customers to get the high-quality, affordable health care they need wherever they are.
- According to Excellus, the information accessed may have included members' name, date of birth, address, telephone number, Social Security number, member identification number, financial account information, and claims information.
- Capital BlueCross systems were not impacted by, and were not part of, the Excellus breach. Capital BlueCross and Excellus are separate and distinct companies.
- 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.
- If you have not received health care services in Excellus' service area Central New York State since 1993 (using the BlueCard network), your information should not be at risk.
- Excellus has established a dedicated call center for its members and other affected individuals: at 877.589.3331.
- Excellus will be notifying all affected members and offering two years of free identity protection services and credit monitoring. Anyone who believes that their information may be involved can enroll in these services, even before receiving the Excellus letter, by enrolling online at www.excellusfacts.com or by phone at 877-589-3331.
- Excellus delayed announcing the cyber-attack until September 9 in order to more clearly determine the individuals potentially affected.

Notification to Affected Members and ASO Group Customers

- On or about September 10, Excellus will begin sending notifications by U.S. mail to impacted Excellus members.
- Impacted members will be provided with two years of free credit monitoring and identity protection services through Kroll.
- 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, with affected members, as we have done in the past. Excellus will send letters to any affected Capital BlueCross member.. More details will be provided as they unfold.
- As with other recent cyber-attacks, a business decision has been made to not to send letters to fully insured groups.
- Any individual who believes they may have been affected by this breach and wants to enroll in these services, prior to receiving their letter, may do so by following the instructions for enrollment found at: www.excellusfacts.com.

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.

Capital BlueCross Member Q&A

Q: Has Excellus provided Capital BlueCross with information indicating that Capital BlueCross members were impacted by the cyber-attack?

- A: Although Capital BlueCross systems were not impacted by, and were not part of, the attack on Excellus, we are working with Excellus to identify any of our members who may have received services in Excellus' coverage area that includes [31 counties in upstate New York](#) since 1993 because their information is potentially affected.
- Our members could be affected because Capital BlueCross is one of 37 independent, locally operated companies across the United States that form the BlueCross BlueShield system. This affiliation enables BlueCross BlueShield system plan customers to get the high-quality, affordable health care they need wherever they are.

- Excellus will send letters to all impacted individuals. More details will be provided as they unfold.
- Impacted members will be provided with two years of free credit monitoring and identity theft protection services.

Q: I am not a member of an Excellus plan. Why could my personal information be impacted?

- A: Any member of a Blue plan who received health care services in Excellus' service area that covers [31 counties in upstate New York](#) since 1993 may have been affected by this attack. 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: When will I receive a letter from Excellus if my information was accessed?

A: If your information was accessed, you will receive a letter from Excellus in the coming weeks. However, if you believe that you have been affected, you do not have to wait to enroll in the identity protection and credit monitoring services. You can enroll in these online through the information at www.excellusfacts.com or by phone at 877-589-3331.

Q: Will producers/consultants receive a copy of the group or member letter?

A: Yes, producers will receive a copy of Excellus' member notification letter and CBC's letter to any impacted current and former ASO groups. The group letters will be addressed to the Policymaker on record for the group.

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

A: Excellus is providing two years of free credit monitoring and identity theft protection services to impacted individuals. Details of this service are included in the letters Excellus is sending to impacted individuals. If any individual believes that their information may have been accessed, they may enroll in the services even if they have not yet received a letter. Instructions for how to enroll are available at www.excellusfacts.com or by calling 877.589.3331.

Q. Is the Excellus data breach related to any other recent breaches at other BlueCross BlueShield system plans?

A. Since these cyber-attacks are still ongoing FBI investigations, we do not have any definitive answer to these questions.

Q. If a member was affected by a data breach at another BlueCross BlueShield system plan, should they sign up for all free credit monitoring and identity theft protection services offered?

A. We encourage members to enroll for services with at least one of the free credit monitoring and identity theft protection providers offered by the plans. If a member already enrolled in other identity protection and credit monitoring services and they are uncertain about the need to enroll with Kroll after the Excellus breach, they should call 877.589.3331 to determine if there is any additional benefit to signing up for a second service.

Q. Can we identify whether or not a member's SSN was breached in the Excellus attack?

A. Unfortunately, we cannot. Although Excellus' investigation has not determined that any information was removed from their systems as a result of the cyber-attack, the attackers did gain unauthorized access to Excellus' IT systems, allowing them to potentially access a wide range of information, including SSNs.

Q: What steps does Capital BlueCross take to protect member information?

A: 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 and equipment, 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.

Q: Where can I find out more information about the attack on Excellus?

A: More information can be found at www.excellusfacts.com.

Consolidated Q&As Provided by Excellus and the BCBSA

Q. How did this happen?

A. Excellus was targeted by this cyber-attack, and national news in recent months has made clear that both the business community and government face significant threats in this area. Excellus worked with Mandiant, one of the world's leading cybersecurity firms, to investigate the attack and remove the infection created by the attack on their IT systems. Along with steps they took to cleanse their IT system of issues raised by this cyber-attack, Excellus is taking additional actions to strengthen and enhance the security of their IT systems moving forward.

Q. Who and how many people have been impacted?

A. The investigation found the attacker accessed Excellus' network and may have accessed personal information related to their members, providers, producers, brokers, employees and other organizations and people with whom they do business. Some of that data goes back to 1980. Approximately ## 10 million individuals are impacted.

Q. What information may have been accessed?

A. The investigation has determined that the attackers may have possibly gained unauthorized access to the following information: name, address, date of birth, telephone number, member identification number, Social Security number, financial account information, and claims information, including clinical information. The information involved dates back to 1980, but information on BlueCard members dates back to 1993. The investigation has not determined that any such data was removed from our systems. They also have no evidence to date that such data has been used inappropriately.

Q. When did the attack happen?

A. Excellus' investigation revealed that the attack may have been initiated on December 23, 2013.

Q. When did Excellus learn of the intrusion?

A. Excellus discovered signs of the cyber-attack on August 5, 2015.

Q. Who discovered the intrusion?

A. Excellus discovered signs of the cyber-attack in collaboration with Mandiant, one of the world's leading cybersecurity firms.

Q. What is the source of the intrusion?

A. That's the subject of an active law enforcement investigation involving the FBI, which they are not able to comment on at this point.

Q. Have any criminals been identified/apprehended?

A. As part of their investigation, Excellus notified the FBI, and they are coordinating with their own investigation into this attack. This investigation is ongoing.

Q. Has the situation been resolved?

A. Excellus has been working with Mandiant, one of the world's leading cybersecurity firms, to investigate the attack and remove the infection from their systems. Along with steps they took to cleanse their IT system of issues raised by this cyber-attack, Excellus is taking additional actions to strengthen and enhance the security of their IT systems moving forward.

Q. Why did it take from August 5 to September 9 to make the announcement?

A. Excellus was working to close the vulnerability on their system, cooperate with the FBI in their investigation and more clearly identify the affected individuals.

Q. What steps has Excellus taken to remediate the issue?

A. Addressing this issue with strengthened IT security and working to provide those affected by this attack with the assistance they need has been a top priority for Excellus. As part of their investigation, Excellus notified the FBI and is coordinating with their own investigation into this attack. The company retained and has been working with Mandiant, one of the world's leading cybersecurity firms, to investigate the attack. They also worked closely with Mandiant to remove the infection created by the attack on their IT systems. Along with steps they took to cleanse their IT system of issues raised by this cyber-attack, Excellus is taking additional actions to strengthen and enhance the security of their IT systems moving forward.