Excellus

Christopher C. Booth
Chief Executive Officer

The Honorable Michael F. Nozzolio
New York State Senate 54th District
119 Fall Street
Seneca Falls, New York 13148

Dear Senator Nozzolio:

Thank you for the opportunity to provide additional information regarding the cyberattack against Excellus BlueCross BlueShield ("Excellus BCBS"). The subject is an important one. We look forward to working with you and other policymakers in addressing the issues and concerns being experienced by constituents as well as the broader topic of ongoing, extensive cybercrime impacting health, education, retail, banking and other industries in the United States as well as our own government.

The criminal attack on Excellus BCBS affects millions of people, including our members, patients, and others with whom we do business. It also affects most of our employees.

Since discovery of the attacker's intrusion, we have taken numerous steps to protect the interests of those potentially impacted parties, including, within days of discovering the attack, involving the Federal Bureau of Investigation (FBI). Our measures have included a comprehensive approach to remediation that has strengthened our Information Technology (IT) security which should mitigate the potential for further intrusion or damage to our systems.

Equally important, we are offering immediate monitoring and restoration services for our members, patients, employees and other potentially affected individuals against credit and identity theft. Our goal throughout the response to this incident was to do what we could do to make this less burdensome for those potentially affected by this criminal attack.

With regard to your specific questions:

1. **How was such an extensive security lapse able to exist undetected for nearly two years?**

   A "security lapse" did not occur. This was a sophisticated cyberattack. The attackers used techniques to actively hide their presence in the environment, which made it more difficult for Excellus BCBS to detect the attack.

2. **Why is the public only being informed of this cyberattack now? Why did Excellus take five weeks to advise its subscribers of the breach once it was discovered on August 5th?**

165 Court Street, Rochester, NY 14647
Telephone: (585) 453-6359 ✦ Facsimilie: (585) 238-4526 ✦ christopher.booth@excellus.com

On August 5, 2015, we learned of the earliest indications of the cyberattack. At that time, we immediately began incident response measures and contacted the FBI. FireEye's Mandiant incident response division ("Mandiant") moved aggressively to scan our IT environment over the next several weeks in order to determine whether there was any active compromise of our IT systems and whether, in fact, there had been any unauthorized access to data. That timeframe also was necessary to remove all malware and backdoors from our IT systems in order to prevent the attacker from using those tools to remotely access our network. We also used that time to implement a number of system enhancements highlighted in our response to your fifth question. Throughout this process, Excellus BCBS was also fully cooperating with the FBI's investigation.

Excellus BCBS's priority throughout has been to determine who, if anyone, was impacted and to get resources and services established to assist those individuals. The services and supports include a dedicated call center, a notification fulfillment vendor, credit monitoring and identity theft resolution services, and incident-specific internet websites for all potentially affected individuals. All of these services needed to be established so that potentially impacted people could get information and assistance immediately upon hearing our announcement. We did not contact individuals before that happened because we had no evidence that any information was actually removed or that information had been used inappropriately. At the same time, the attack did not disrupt any services or impact the integrity of Excellus BCBS's data.

3. **How was this attack discovered? What incident/event prompted its discovery?**

As a result of cyberattacks on other insurance companies across the country, Excellus BCBS proactively engaged Mandiant, one of the world's leading cybersecurity firms, to conduct a forensic assessment of all of its IT systems. During that assessment, Mandiant discovered indications that a cyberattack occurred.

4. **Was the attack of December 23, 2013 the sole attack, or have there been other incidents of unauthorized access? If so, how many and when? And most importantly, did the hackers have prolonged access to confidential data within the Excellus system during the past 20 months?**

The investigation revealed that the earliest evidence of the attack occurred on December 23, 2013. The last evidence of attacker activity in the Excellus BCBS environment was on August 18, 2014. The last evidence of the attackers potentially having access into the Excellus BCBS environment was May 11, 2015. There have been no other incidents of unauthorized access and there is no evidence that any sensitive data was actually removed from our network.

5. **Prior to this attack, did Excellus proactively engage the services of expert cybersecurity firms of Mandiant's stature to conduct periodic vulnerability assessments and penetration testing?**

Yes, over the years, Excellus has retained a series of reputable vendors to conduct penetration testing on an annual basis. Excellus also purchased industry leading vulnerability assessment

tools which it runs on a regular basis in its environment. As many companies are learning from sophisticated attacks, these services may not always identify a compromise.

What assurances can you provide to the public that Excellus has committed sufficient resources and taken other necessary actions to strengthen the security of its information technology systems?

We have acted aggressively in response to this attack, including dedicating substantial resources to strengthen the security of our systems. Specifically, Excellus BCBS has removed all malware and backdoors from its IT systems in response to this cyberattack, which has prevented the attacker from using those tools to remotely access Excellus BCBS's network. Consistent with Mandiant's recommendations, Excellus BCBS has implemented a number of system enhancements, including among others:

- Identifying all privileged network accounts and changing passwords for those accounts, as well as changing database administrators' passwords and Active Directory credentials;
- Enhancing and expanding our security and system event logging capabilities;
- Installing enhanced monitoring tools to detect any new or potential attack;
- Continued auditing of the use of two-factor authentication for remote access; and
- Escalating an existing project to monitor databases with sensitive data.

6. **If a breach does occur in the future, has Excellus instituted the appropriate systems and procedures to rapidly detect and rapidly respond to such an event?**

Yes. Security of the information we maintain and appropriate and planned incident response procedures should an event occur will remain one of our top priorities. Excellus BCBS is continuing efforts to improve those controls and has instituted appropriate systems and procedures to rapidly detect and respond to security incidents.

7. **Is the investigation by Excellus/Mandiant into the unauthorized access of subscriber data concluded, or is it continuing?**

Our investigation is ongoing, but in the final stages. Our investigation has not determined that any sensitive data was removed from our IT systems and to date there is no evidence that any data has been used inappropriately.

8. **To what degree of confidence did the Excellus/Mandiant investigation reveal that NO DATA was removed, copied, altered, sold or otherwise utilized by the attackers?**

We have confirmed that there is no evidence in Excellus's network that any sensitive data was removed from Excellus BCBS's systems. The confirmation of this fact was important for the timing of our communications as well. We did not want to provide information that later was

deemed to be inaccurate. Excellus BCBS, through its work with Mandiant as well as the FBI, is not aware of any evidence to date that such data has been used inappropriately. As noted above, Excellus BCBS's computer network has been remediated to remove all malware and backdoors from its IT systems in response to this cyberattack. However, because Excellus BCBS could not conclude with certainty that information was not accessed, we offered the monitoring and identity theft protection services through Kroll.

9. **Did your investigation uncover whether all of Excellus' subscribers were subjected to the cyberattack, or identifiable subsets?**

Although Mandiant and Excellus did not find evidence of the collection or exfiltration of sensitive data, the attackers may have had the means and the capability to access the sensitive data of all of Excellus' members. Due to the way that our network was configured, with some data segregated and stand-alone authentication for certain systems, there were identifiable subsets that were deemed to be not at risk.

10. **Does Excellus have information about the nature and extent this data was accessed?**

Although our network was accessed by the attackers, we have not determined that any sensitive information was actually accessed. Since they had the capability of accessing certain sensitive information, we are letting those potentially impacted know that this happened and the steps they can take to protect themselves.

11. **Is this portion of Excellus' investigation concluded, or is it continuing?**

Our investigation is in the final stages and nothing has changed from our initial announcement.

12. **Additionally, the online edition of WIRED magazine reported on September 10, 2015: "Excellus says that it did encrypt that sensitive information. But it doesn't seem to have done so in a way that would prevent hackers from seeing it. Excellus spokesperson Cane [sic] [Kevin Kane] told WIRED that because the hackers had gained administrative access to the company's network, they would be able to circumvent its encryption, likely by accessing decryption keys available to administrators. According to this report, not only were hackers able to access Excellus' servers, but they were also able to penetrate Excellus' administrative network in order to obtain its encryption key, which would allow for the confidential, private medical and other personal information of the subscribers and others to be read by the hackers. Is this report accurate? What security measures were in place to protect this encrypted information and the key to decode that information through the Excellus administrator network? If proper security measures were in place, how were the hackers able to penetrate the encryption employed and also gain access to Excellus' information sharing partners?**

We use various types of encryption in our business processes. Ultimately, most of the databases affected were not encrypted and, even if they had been, because of the type of access the attacker possibly had in the environment, encryption would not have blocked this type of attack. To clarify, there is no evidence that the attackers were able to "gain access to

Excellus' information sharing partners." This event did not involve a virus. The malware used by the attackers cannot be passed from one network to another without attackers intentionally inserting the malware into the second network. Further, working with Mandiant, we removed the malware used by the attackers on our IT systems and the attack has been blocked.

13. **You indicated in your public statement "This incident affects members, patients, or others who have done business with the impacted plans listed below." Please clarify what groups of people/organizations are included in your reference to "others who have done business with the impacted plans".**

The others who would have done business with the impacted plans would include certain vendors, brokers and providers who supplied us with Tax ID numbers that matched a valid Social Security Number. We are notifying those affected individuals.

14. **Is Excellus indicating that confidential information of every hospital, pharmacy, physician, and other type of medical provider affiliated with its network might be impacted by this cyberattack?**

No.

15. **Does this mean the confidential information of every employee, vendor, independent contractor and supplier who provides Excellus with goods and services for its varied day-to-day operations might have been accessed?**

No.

16. **When do you expect Excellus to further identify these entities and communicate to those victims who were impacted by this attack?**

The individuals potentially impacted by this cyberattack have been identified. We began mailing letters to those people on September 9, 2015. We plan to complete mailing most of the letters in the next few weeks. In some instances, where we need to further research and validate current address information for potentially impacted individuals, including those who are members of other Blue Plans, those letters will be mailed no later than the notification period permitted by HIPAA. In the meantime, individuals who believe they are affected by the cyberattack do not need to wait for their letter to sign up for the two years of complimentary credit monitoring and identity theft protection services. They can enroll by visiting excellusfacts.com and clicking on the "ACTIVATE FREE CREDIT MONITORING NOW" link in the upper right-hand corner of the website.

17. **How does Excellus plan to monitor the services its subcontractors Kroll and TransUnion provide to those subscribers and others impacted by the breach?**

We have secured the services of Kroll to provide identity theft protection at no cost to affected individuals for two years, including two years of credit monitoring services powered by TransUnion. These services include Credit Monitoring, Web Watcher, and Identity Theft

Consultation and Restoration. We actively supervise Kroll and our team has a daily call with the Kroll team to address any issues that may arise.

18. **What reports is Excellus requiring of these service providers? Will the reports be made public to the Excellus subscribers and all other individuals who may have had their confidential personal information compromised by this cyberattack?**

Kroll provides Excellus BCBS with a daily updates regarding its call center and activations of services. Tens of thousands of people have enrolled in the services so far. We have gone to great lengths to inform and educate affected individuals about this incident, including issuing a nationwide press release, establishing a dedicated website and call center, and responding to affected individuals' questions on social media. These actions are in addition to the direct mailings to millions of people. Our goal is to make sure affected individuals get the tools and assistance they need to protect themselves.

Senator, I appreciate your interest in this incident. Please be assured that we are taking this issue very seriously. We are dedicated to addressing any issues that potentially impacted individuals may have. Please let me know if you have further questions or if you would like to meet to discuss these issues.

Sincerely,

Christopher C. Booth
President and CEO
Excellus BlueCross BlueShield