THE SENATE
STATE OF NEW YORK

CHAIRMAN
CODES

CO-CHAIRMAN
NYS LEGISLATIVE TASKFORCE ON
DEMOGRAPHIC RESEARCH & REAPPORTIONMENT

COMMITTEES
FINANCE
RULES
CRIME & CORRECTIONS
ELECTIONS
HOUSING
INVESTIGATIONS
JUDICIARY
RACING & WAGERING
TRANSPORTATION

SENATOR
MICHAEL F. NOZZOLIO
54TH DISTRICT
MAJORITY WHIP OF THE SENATE

September 2015

Mr. Christopher C. Booth, President & CEO
Excellus BlueCross BlueShield
165 Court Street
Rochester, New York 14647

Dear Mr. Booth:

As Chairman of the New York State Senate Codes Committee, Chairman of the Senate Public Protection Budget Subcommittee with jurisdiction over our State's Homeland Security budget, and the New York State Senator representing six counties in the Finger Lakes region, the home of thousands of Excellus BlueCross BlueShield subscribers, it is with great concern that I am writing to you regarding the cyberattack on Excellus and related companies, as announced in your public statement of September 9, 2015.

This massive security breach raises many important questions that, to date, remain unanswered. You indicated the attack on Excellus' data systems has been investigated internally by the company and externally referred by Excellus to the appropriate law enforcement officials. A major concern is that even with the essential first steps taken, Excellus' public response has not been sufficiently transparent, nor comprehensive. Victims of this cyberattack simply have not been provided with adequate information about the scope and nature of the unauthorized access of their confidential personal and medical information, nor have they been assured all necessary steps are being taken to prevent this from happening again.

It is common knowledge in today's world that cyberattacks are a very real and constant threat, having the potential to disrupt lives, destroy good credit, take much time and effort to unravel and, in some cases, alter lives indefinitely.

-continued-

Seneca Falls: 119 Fall Street, Seneca Falls, NY 13148 • (315) 568-9816 • FAX: (315) 568-2090
Albany: Room 503, Capitol, Albany, NY 12247 • (518) 455-2366 • FAX: (518) 426-6953
Toll Free # 1-888-568-9816
www.nozzolio.nysenate.gov • nozzolio@nysenate.gov

Because of the highly confidential, sensitive and personal nature of information with which Excellus is entrusted and required to protect, this large-scale security breach is much more personally invasive to its individual victims, the Excellus subscribers, than other cyberattacks reported in recent years. On behalf of my constituents I raise to you the following questions, and respectfully implore your prompt attention and response:

- Excellus indicated it learned of the security breach on August 5, 2015, and the "initial attack" occurred on December 23, 2013. How was such an extensive security lapse able to exist undetected for nearly two years? Why is the public only being informed of this cyberattack now?

- How was this attack discovered? What incident/event prompted its discovery? Why did Excellus take five weeks to advise its subscribers of the breach once it was discovered on August 5th? 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?

- Your public statement about the attack indicated Excellus has: *"...worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remediate the issues created by the attack on our IT systems. We are taking additional actions to strengthen and enhance the security of our IT systems moving forward."* These are positive steps, but they also raise other important questions. 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? 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? 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?

-continued-

- Your public statement indicated: *"The investigation has not determined that any such data was removed from our systems. We also have no evidence to date that such data has been used inappropriately."* Is the investigation by Excellus/Mandiant into the unauthorized access of subscriber data concluded, or is it continuing? 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?

- Your public statement indicated: *"Our investigation determined that the attackers may have gained unauthorized access to individuals' information, which could include name, date of birth, Social Security number, mailing address, telephone number, member identification number, financial account information and claims information."* Did your investigation uncover whether all of Excellus' subscribers were subjected to the cyberattack, or identifiable subsets? Does Excellus have information about the nature and extent this data was accessed? Is this portion of Excellus' investigation concluded, or is it continuing?

- 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?

-continued-

- You indicated in your public statement *"This incident affects members, patients, or others who have done business with the impacted plans listed below."* The scope of those impacted could be extremely large in number. Please clarify what groups of people/organizations are included in your reference to *"others who have done business with the impacted plans"*. 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? 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? When do you expect Excellus to further identify these entities and communicate to those victims who were impacted by this attack?

- Excellus is providing two years of "free credit monitoring and identity theft protection services" to its subscribers. Hopefully the services provided by Excellus through vendors Kroll and TransUnion will be helpful to those affected, even though the security breach first occurred almost two years ago. How does Excellus plan to monitor the services its subcontractors Kroll and TransUnion provide to those subscribers and others impacted by the breach? 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?

It is my hope you share the belief that it is vitally important for Excellus to provide subscribers and others impacted by this data breach with answers to these essential questions. Thank you for your time and attention to this important matter.

Sincerely,

Michael F. Nozzolio

Michael F. Nozzolio
Senator, 54th District