

March 27, 2015

The Honorable Patty Murray  
United States Senate  
Committee on Health, Education, Labor, and Pensions  
428 Senate Dirksen Office Building  
Washington, DC 20510-6300

*Transmitted via email*

Dear Senator Murray:

Thank you for your letter of March 20, 2015 expressing interest in learning more about the cyberattack against Premera Blue Cross. This letter provides additional information on that unfortunate incident.

This criminal attack on Premera affects millions of people, including our members, employer customers, providers and others with whom we do business. Since discovery of the attacker's intrusion, we have taken every step possible to protect the interests of those impacted parties. Our measures have included a pragmatic approach to remediation that strengthened our Information Technology (IT) security against potential for further intrusion or damage to our systems prior to public notification. As important, we have offered immediate protections for our members against credit and identity theft. As much as possible, we have sought to make this criminal event our burden, not that of individuals affected by this incident.

Premera has also coordinated closely with the Federal Bureau of Investigation (FBI). While working with law enforcement, we also look forward to supporting policymakers in addressing the broader issue of cyber security and cybercrime in the United States.

The balance of this letter provides answers to your questions.

**1. When will Premera complete efforts to notify the 11 million affected current and former policy holders?**

Of the 11 million affected individuals, approximately 6.5 million are current or former members, employer customers, providers, employees and other organizations and people with whom Premera does business. Of that, approximately 6 million are current and former policyholders of Premera or its affiliates.

Premera began mailing notification letters to affected individuals on the day of our announcement, March 17, and is proceeding with notification as expeditiously as possible. We anticipate all letters to current and former Premera members will be mailed by March 30. Additionally, Premera is coordinating with other Blue Cross Blue Shield plans across the

country to communicate with members of those plans who may be affected because they may have received medical services in Washington or Alaska. We anticipate that all letters to affected individuals will be mailed by mid-April.

**2. Why did Premera not immediately disclose the breach to the Department of Health and Human Services' Office of Civil Rights as required by HIPAA?**

Mandiant, one of the world's leading cyber security firms, was engaged by Premera to assist it in investigating the cyberattack. Mandiant strongly cautioned Premera that sending notifications to members or publishing media notice, or implementing incomplete remediation before the scope of the intrusion was determined, would alert the attackers and could prompt them to download sensitive information, further embed themselves in the system or otherwise do further harm to both Premera and its members. We followed Mandiant's advice in the interest of protecting our ability to serve our customers and to better protect their personal information.

In addition, I should clarify that under HIPAA, a covered entity such as Premera, is not required to notify the Office for Civil Rights immediately of an incident. Rather, a covered entity is required to notify the Office for Civil Rights of an incident at the same time the covered entity notifies affected individuals, but in no event later than 60 days from the discovery of the incident. 45 C.F.R. § 164.408(b). Accordingly, Premera complied with applicable HIPAA requirements when it notified the Office for Civil Rights on March 17 of the cyberattack we discovered on January 29.

**3. Why did Premera not immediately inform the 11 million current and former policy holders that their personal, financial and health records have potentially been compromised?**

As noted above, Mandiant warned Premera about the dangers of making any public announcement about the attack until the following steps could be taken: 1) Mandiant completed scanning all servers and workstations for areas of infection to identify all attack vectors; 2) systems were remediated in a concentrated time to lock the attackers out of system; and, 3) remediation was followed by scanning to verify that the all backdoors were eliminated.

As Mandiant explained, the reason that these steps were necessary is that any public announcement would also alert the attackers themselves, and that the attackers could have then taken any of the following steps before they lost access to the network: downloading sensitive information from the network; corrupting data; disrupting network service; and creating new vulnerabilities and further embedding themselves in the system, making it even more difficult to eradicate the attackers and prolonging their access to sensitive information.

Accordingly, Premera made the decision to complete the remediation efforts to eliminate all malware and backdoors and to validate that Premera had secured its IT systems before the public notice of the attack. This is consistent with applicable Washington state law that recognizes that a company may need to remediate its systems prior to notice to affected individuals. See RCW 19.255.010(1).

**4. What steps will Experian now that it is retained by Premera take to help affected individuals not just monitor but repair credit if necessary?**

The Experian services being provided by Premera at no cost to affected individuals include two free years of credit monitoring, identity protection services, as well as identity theft insurance. Specifically, those services include access to professional Fraud Resolution agents who specialize in working directly with individuals from beginning-to-end to help repair credit and resolve identity theft. The services also include ExtendCare, which continues the individual's access to Fraud Resolution agents even after the two year complimentary ProtectMyID enrollment has ended. Among other forms of assistance, Fraud Resolution agents can help by:

- Placing a temporary 90-day or extended seven-year fraud alert on consumers' Experian credit reports, as requested, to help stop fraudulent new accounts from opening;
- Sharing the fraud alert with the Equifax® and TransUnion® credit bureaus;
- Assisting with the dispute process for inaccurate information or fraudulent activity on Experian credit reports;
- Drafting and providing dispute letters for members to report credit fraud to Equifax and TransUnion;
- Assisting in scheduling conference calls with financial providers, creditors, and service providers to dispute fraudulent charges and accounts;
- Interacting with law enforcement or government agencies to work toward a resolution and assist with filing a police report, if possible;
- Providing copies of all necessary letters to report credit fraud and identity theft to creditors, credit reporting agencies or others who may be involved in the process of reclaiming the member's identity; and
- Reviewing credit records to help members determine potential areas of fraud.

**5. What steps is Premera taking to assist Washington businesses that offer plans through Premera to address security risks arising from the breach?**

Mandiant determined that the malware from the cyberattack could not pass from Premera to other organizations with which Premera exchanges information electronically, such as providers, employers, or members. Therefore, the IT systems of these businesses were not impacted by the cyberattack on Premera.

**6. What steps is Premera taking to reduce and protect against risks of cyber incursions at companies whose employees are insured through Premera?**

Given that this cyberattack was not a virus, the IT systems of companies whose employees are insured through Premera were not impacted by the cyberattack on Premera.

**7. What were the findings of outside security consultant Mandiant?**

Mandiant's investigation to date has identified only intrusion but no exfiltration of information from Premera's systems. Mandiant has not conclusively determined the initial vector of compromise. That is, they don't know if the malware came from a phishing email, a contaminated website, or another source of intrusion.

**8. How was the breach discovered?**

Premera retained Mandiant to perform a proactive compromise assessment of Premera's IT network given the number of publicly reported cyberattacks against other private sector businesses earlier in 2014. The attack was discovered during this assessment.

**9. How were the attackers able to penetrate the entire Premera system?**

Upon penetration of Premera's network, the attackers gained access to log-in credentials and then deployed other tools and tactics to gain broad access to Premera's network.

**10. Were the attacks on Premera and Anthem connected and which company was attacked first?**

Premera is not in a position to opine about whether the Premera and Anthem attacks were connected or which attack occurred first. Because these attacks are the subject of active FBI investigations, Premera encourages your office to contact the FBI for additional information.

**11. While Premera officials have stated that data was not moved off the Premera system can you be certain that data that was accessed cannot be used for malicious purposes?**

Mandiant's investigation has not determined that any of the potentially affected data was removed from Premera's systems. In addition, Premera is not aware of any evidence to date that such data have been used inappropriately. As noted above, the Premera computer network has been remediated to remove all malware and backdoors.

Since Premera cannot be certain that information that may have been accessed could not be used for malicious purposes, Premera has implemented the credit monitoring and identity protection services from Experian described in question 4, above.

**12. Please explain how Premera uses the National Institute of Standards and Technology health care cyber security framework to implement and evaluate its cyber security.**

We use the National Institute of Standards and Technology (NIST) health care cyber security framework as one of the guidelines for establishing the policies and procedures that guide our cyber security efforts.

**13. Why did Premera opt not to be certified by the Health Information Trust Alliance (HITRUST) and in what ways did Premera's systems fail to meet the requirements for HITRUST certification?**

HITRUST is a private certification process that is not a requirement under any federal or state law, nor a requirement of any federal or state program in which Premera participates. Premera has not pursued HITRUST certification and thus has not been evaluated against its criteria.

**14. What steps did Premera take to improve cyber security to address issues raised in the 2014 audit by the Office of Personnel Management?**

The Office of Personnel Management ("OPM") report dated November 28, 2014, reached the following overall conclusions about Premera's IT security (quoting directly from the report):

- "Nothing came to our attention to indicate that Premera does not have an adequate security management program."
- "Nothing came to our attention that caused us to believe that Premera is not in compliance with the HIPAA security, privacy, and national provider identifier regulations."

As is common with audits, the report identified areas for improvement, and we have taken those seriously. Premera implemented most of the items identified by OPM in 2014 and will be implementing all the recommendations this year.

Mandiant found no evidence that the cyberattack on Premera was the result of, or was related to, any of the items identified in the OPM report.

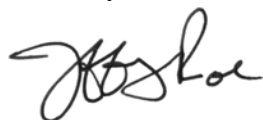
**15. What additional steps will Premera be taking to improve security going forward?**

Premera removed all malware and backdoors from its IT systems in response to this cyberattack. Consistent with Mandiant's recommendations, Premera has implemented a number of system enhancements, including among others:

- Deploying multiple-factor authentication for remote access to Premera's network;
- Scanning servers, desktops, and laptops as a requirement for continued use of devices on the network;
- Installing enhanced monitoring tools to provide reports of any new attacks on our computer networks;
- Enhancing and expanding our security and system event logging capabilities; and
- Engaging a service provider for advanced monitoring services.

Again, I appreciate your interest in this incident and efforts to strengthen cyber security in the United States. Please let me know if you have any further questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Jeffrey Roe". The signature is fluid and cursive, with the first name "Jeffrey" being more prominent than the last name "Roe".

Jeffrey Roe  
President and CEO