

Premera Blue Cross Cyber-Attack

Producer Communication #705

Issued March 19, 2015

Updated April 9, 2015

Message

On March 17, 2015, Premera Blue Cross announced that the company was the victim of a cyber-attack during which attackers gained unauthorized access to Premera's information technology system. The attack was discovered on January 29, 2015 and the subsequent investigation revealed that the initial attack occurred on May 5, 2014 and involves information that dates back to 2002.

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

Details

Since learning of the Premera cyber-attack, Capital BlueCross has been working diligently to gather information about the attack on Premera and how it might impact any of our members.

The Premera attack involved the information of members of other BlueCross and BlueShield plans who sought treatment in Premera's service area, which includes Alaska and Washington State. That is because 37 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 Premera's service area in Alaska and Washington State since 2002, their information should not be at risk.

As part of its investigation, Premera notified the FBI and is coordinating with the Bureau's investigation into this attack. Premera 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.

According to Premera, 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, and claims information, including clinical information. No credit card or financial information was included. More information about this incident can be found at www.premeraupdate.com.

Letters will be mailed to all affected individuals and they will be provided with two years of free credit monitoring and identity theft protection services.

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.premeraupdate.com.

Premera delayed announcing the cyber-attack until March 17 after receiving strong advice that they should first block the attack and cleanse their IT systems. This delay was to prevent the attackers from engaging in even more malicious activity and prevent greater risk to impacted members.

Notification to Affected Members and ASO Group Customers

On or about April 10, Premera plans to begin sending notifications by U.S. mail to members, including Capital BlueCross members, whose information was accessed. There are two versions of these

notifications; one for impacted adults and one for children under the age of 18 at the time of the mailing, whose information was impacted.

On Wednesday, April 8, Capital BlueCross sent letters to ASO group customers that have affected members to provide advance notice that their affected members will receive notification from Premera by U.S. mail. The letter directs active ASO groups with questions to contact their account executive or producer (*Attachment C*). A listing of the group's current and/or former members that were affected by the Premera breach and a copy of Premera's member notification letters were included as enclosures (*Attachment D*).

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 1.866.814.7544. 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 E*) and the copy of Premera's member notification letters will be included as enclosures (*Attachment D*).

A business decision has been made to not to send letters to fully insured groups. Other plans have reported that they are following the same course.

- If another BlueCross BlueShield system plan served as the affected group customer's administrator since 2002, groups may receive a letter from that plan in addition to the letter we are sending; however, affected customers will only receive one notification from Premera.
- ASO groups may have members who receive a Premera 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 2002 that was administered by another BlueCross BlueShield system plan, such as one that may have been offered through a different employer.
- HITECH Breach Notification and HHS – Premera 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. Premera's 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

Health care benefit programs issued or administered by Capital BlueCross and/or its subsidiaries, Capital Advantage Insurance Company®, Capital Advantage Assurance Company® and Keystone Health Plan® Central. Independent licensees of the Blue Cross and Blue Shield Association. Communications issued by Capital BlueCross in its capacity as administrator of programs and provider relations for all companies.

Producer Bulletin



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** – **Premera Talking Points and Q&A**
- **Attachment B** – Capital's Premera Statement
- **Attachment C** – Capital's Premera Letter to current ASO groups
- **Attachment D** – Premera's Letters to affected members
- **Attachment E** – Capital's Premera Letters to former ASO groups
-

Questions

Contact your Preferred Agency with any questions. Thank you.

PREMERA BLUE CROSS TALKING POINTS and Q&As

April 2015

Talking Points

- On January 29, 2015, Premera Blue Cross discovered that cyber attackers executed a sophisticated attack to gain unauthorized access to Premera's information technology system.
- Premera discovered signs of the cyber-attack in collaboration with Mandiant, one of the world's leading cybersecurity firms.
- Premera's investigation revealed that the initial attack occurred on May 5, 2014.
- The information involved in the Premera incident dates back to 2002 and impacts nearly 11 million individuals.
- The Premera attack involved the information of members of other BlueCross and BlueShield plans who sought treatment in Premera's service area, which includes Alaska and Washington State.
- 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 Premera, the information accessed may have included members' name, date of birth, address, email address, Social Security number (only if it is part of a member's identification number or patient identifier), telephone number, member identification number, and claims information, including clinical information. No credit card or financial information was included.
- Capital BlueCross systems were not impacted by, and were not part of, the Premera breach. Capital BlueCross and Premera Blue Cross are separate and distinct companies.
- Since learning of the Premera cyber-attack, Capital BlueCross has been working diligently to gather information about the attack on Premera and how it might impact any of our members.
- If you have not lived in and/or received health care services in Premera's service area in Alaska and Washington State since 2002, your information should not be at risk.
- Premera has established a dedicated call center for its members and other affected individuals: at 1-800-768-5817 (M-F 8:00am-11:00pm Eastern Daylight Time.)
- More information can be found at: www.premeraupdate.com.
- Premera delayed announcing the cyber-attack until March 17 after receiving strong advice that they should first block the attack and cleanse their IT systems. This delay was to prevent the attackers from engaging in even more malicious activity and prevent greater risk to impacted members.

Notification to Affected Members and ASO Group Customers

- On or about April 10th, Premiera will begin sending notifications by U.S. mail to members, including Capital BlueCross members, whose information was accessed.
- Impacted members will be provided with two years of free credit monitoring and identity theft protection services through Experian.
- There are two versions of these letters. One is for affected adults and one for affected children, under the age of 18 at the time of the mailing. Adults will be offered Experian's ProtectMyId Alert program and children under the age of 18 will be offered the Experian's FamilySecure program.
- On Wednesday, April 8, Capital BlueCross sent letters to ASO group customers that have affected members to provide advance notice that their affected members will receive notification from Premiera by U.S. mail.
- Active ASO group customers will receive a listing of the group's current and/or former members that were affected by the Premiera breach.
- Former ASO group customers 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 1.866.814.7544. A team of Customer Service representatives is prepared specifically to address calls generated by the letter to former ASO groups.
- A business decision has been made to not to send letters to insured groups. Other plans have reported that they are following the same course.
- If another BlueCross BlueShield system plan served as the affected group customer's administrator since 2002, 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 Premiera.
- ASO groups may have members who receive a Premiera 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 2002 that was administered by another BlueCross BlueShield system plan, such as one that may have been offered through a different employer.
- HITECH Breach Notification and HHS – Premiera 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. Premiera's 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.
- 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.premeraupdate.com.

Capital BlueCross' Commitment to Information Security

- Protecting member information is of the utmost importance to Capital BlueCross.
- Capital BlueCross maintains 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 Premera 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 Premera, findings from Premera's investigation into the attack on its system have identified Capital BlueCross members -- who received health care services dating back to 2002 in areas Premera serves -- whose information was accessed. Premera's service area includes Alaska and Washington State.

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.

Premera is sending notifications by U.S. mail to affected members, including Capital BlueCross members, whose information was accessed.

Impacted members will be provided with two years of free credit monitoring and identity theft protection services.

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

A: Any member of a Blue plan who received health care services in Alaska or Washington State since 2002 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 Premera if my information was accessed?

A: If your information was accessed, you will receive a letter from Premera within the next couple of weeks.

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

A: Premera 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 Premera 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.premeraupdate.com.

Q. Are the Anthem and Premera data breaches related? Were the same attackers involved in both breaches?

A. We know there were some differences in terms of the timing of the breaches and methods of access, but since both breaches are still ongoing FBI investigations, we do not have any definitive answer to these questions.

Q. If a member was affected by both the Anthem and the Premera data breaches should they sign up for both 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, All Clear ID or Experian. If a member already enrolled with All Clear ID as a result of the Anthem breach, and they are uncertain about the need to enroll with Experian after the Premera breach, they should call Experian 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 Premera attack?

A. Unfortunately, we cannot. Although Premera's investigation has not determined that any information was removed from their systems as a result of the cyberattack, the attackers did gain unauthorized access to all of Premera's IT systems, allowing them to potentially access a wide range of information. For purposes of notification, Premera must therefore notify individuals that any information that Premera may have had on its systems, including SSNs, may have been impacted.

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 Premera?

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

Consolidated Q&As Provided by Premera and the BCBSA

Q. How did this happen?

A. Premera 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. Premera 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, Premera 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 Premera's 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 2002. Approximately 11 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 provided to Premera through the BlueCard system: name, address, email address, date of birth, telephone number, member identification number, Social Security number (only if it is part of a member's identification number or patient identifier), and claims information, including clinical information. Information that Premera received through the Blue Distinction Total Care program may also have been accessed. The information involved dates back to 2002. 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. Premera's investigation revealed that the attack may have been initiated on May 5, 2014.

Q. When did Premera learn of the intrusion?

A. Premera discovered signs of the cyber-attack on January 29, 2015.

Q. Who discovered the intrusion?

A. Premera 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, Premera 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. Premera 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, Premera is taking additional actions to strengthen and enhance the security of their IT systems moving forward.

Q. Why did it take from January 29 to March 17 to make the announcement?

A. Premera based its announcement decision on strong advice that they should block the attack and cleanse their IT systems before the announcement. They were warned that other organizations affected by such incidents that ignored this advice experienced the attackers engaging in even more malicious activity. That means affected individuals would have been at greater risk had Premera announced before finishing its investigation and enhancing its IT security.

Q. What steps have Premera taken to remediate the issue?

A. Addressing this issue with strengthened IT security and providing those affected by this attack with the assistance they need has been a top priority for Premera. As part of their investigation, Premera 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, Premera is taking additional actions to strengthen and enhance the security of their IT systems moving forward.

Q. What has Premera done to improve their IT security?

A. Mandiant assisted Premera in a thorough investigation to identify and remove the infection from their systems. They rebuilt a large portion of their IT infrastructure and took additional steps to enhance the security of their system, including: deploying multiple-factor authentication, installing enhanced monitoring tools, and enhancing and expanding security and system event logging capabilities.

Premera Cyber-Attack Update

On March 17, 2015, Premera Blue Cross announced that the company was the victim of a cyber-attack during which attackers gained unauthorized access to Premera's information technology system.

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

However, the Premera attack involved the information of members of other BlueCross and BlueShield plans who sought treatment in Premera's service area, which includes Alaska and Washington State. That is because 37 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 you have not received health care services in Premera's service area in Alaska and Washington State since 2002, your information should not be at risk.

The information involved in the Premera incident dates back to 2002. According to Premera, attackers may have gained unauthorized access to members' information, which for any of our affected members, could include name, date of birth, address, Social Security number, member identification number, and claims information, including clinical information. No credit card or financial information was included. More information about this incident can be found at www.premeraupdate.com.

Letters will be mailed to all affected individuals and they will be provided with two years of free credit monitoring and identity theft protection services. 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.premeraupdate.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.

April XX, 2015

[Current ASO Group Policymaker Name]
[Current ASO Group Policymaker Title]
[Current ASO Group Name]
[Street Address]
[City], [State] [Zip]

Re: Premera Breach Notification

Dear [Current ASO Customer],

On March 17, 2015, Premera Blue Cross announced that the company was the victim of a cyber-attack during which attackers gained unauthorized access to Premera's information technology system. The attack was discovered on January 29, 2015 and the subsequent investigation revealed that the initial attack occurred on May 5, 2014. Premera delayed notification about this attack based on strong advice that Premera first block the attack and cleanse their IT system before any public notification to prevent any additional malicious activity or any greater risk to affected members.

Premera notified the FBI and is fully cooperating with the Bureau's investigation into this attack. Premera 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. Premera continues to work with Mandiant to further strengthen the security of Premera's systems.

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

The Premera attack involved the information of members of other BlueCross and BlueShield plans who live in and/or sought treatment in Premera's service area, which includes Alaska and Washington State. That is because 37 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 lived in and/or received health care services in Premera's service area in Alaska and Washington State since 2002, their information should not be at risk. More information about this incident can be found at www.premeraupdate.com.

Affected Plan Members

Findings from Premera's investigation into the attack have identified current and/or former members of your group health plan whose information was accessed. According to Premera, the information accessed may have included name, date of birth, address, telephone number, email address, Social Security number, member identification number, and claims information, including clinical information.

A list of affected current and/or former members of your group health plan is enclosed.

Notification by Mail to Affected Members

During the next several weeks, Premera is sending notification by U.S. mail to your members whose information was accessed. Each affected member will be provided with two years of free credit monitoring and identity theft protection services.

There are two versions of Premera's notification to affected members- one for adults and one for minors under the age of 18 at the time of the mailing. Copies of both notifications are enclosed.

Important notes concerning our letter to you and Premera's notification to affected members:

- If another BlueCross BlueShield system plan has served as your plan administrator at any time since 2002, you may receive a letter from that plan in addition to this letter. However, affected members will only receive one notification from Premera.
- You may have members who receive a Premera notification who were not covered by your ASO group plan administered by Capital BlueCross. This may be because those individuals were enrolled in another plan at some point since 2002 that was administered by another BlueCross BlueShield system plan, such as one offered through a different employer.

HITECH Breach Notification and HHS

Premera 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. Premera's notification to HHS will cover all affected BlueCross BlueShield system plans and their self-funded group health plans, so there is no need for your plan to make a separate notification to HHS.

Identity Protection Services for Members

Premera is working with Experian, a leading identity protection provider, to offer two years of free identity theft repair and credit monitoring services to all current and former BlueCross and BlueShield plan members whose information was affected. Affected adult members will be offered Experian's ProtectMyID Alert and affected minors under age 18 will be offered Experian's FamilySecure. Any individual who believes they may have been affected by this attack and wants to enroll in these services prior to receiving their letter, may do so by following the instructions for enrollment found at: www.premeraupdate.com.

Toll-Free Hotline for Members

Premera has established a dedicated toll-free number that members can call if they have questions related to this incident. The number is 1.800.768.5817 and it is open Monday through Friday, between 8:00 a.m. and 11:00 p.m. Eastern Daylight Time.

Additionally, consumers may contact the Pennsylvania Attorney General's Health Care Section Helpline at 1.877.888.4877 or 717.705.6938 for further assistance.

Capital BlueCross' Commitment to Information Security

Again, Capital BlueCross systems were not impacted by, and were not part of, the attack on Premera.

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.

We are Here to Answer Your Questions

We understand that the Premera attack and the information shared in this letter may cause concern and generate questions – and we are here to help. If you have questions, please contact your Capital BlueCross account executive or producer. We will provide you with responses as quickly as possible.

As always, we are committed to continuing to serve you and your plan with excellence.

Sincerely,

Tracy Onorofsky
Senior Vice President, Commercial Group Sales



BLUE CROSS

An Independent Licensee of the Blue Cross Blue Shield Association

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<First Name>> <<Last Name>>
<<Street Address>>
<<City>>, <<State>> <<Zip Code>>

<<Date>>

Dear <<FirstName>> <<LastName>>:

I am writing to inform you that Premera Blue Cross ("Premera") was the target of a sophisticated cyberattack, and that some of your personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are coordinating with their own investigation into this attack.

We at Premera take this issue seriously and regret the concern it may cause. I'm writing to provide you information on the steps we are taking to protect you and your information moving forward.

What happened?

On January 29, 2015, we discovered that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on May 5, 2014. We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remove the infection created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your information, which could include your name, address, telephone number, date of birth, member identification number, Social Security number if it is part of your member identification number or patient identifier, email address if you provided it to us, and claims information, including clinical information. 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.

Why does Premera have your information?

We believe you have or had health plan coverage through another independent Blue Cross Blue Shield (BCBS) plan, and that you may have received services in Washington or Alaska at some point since 2002. Premera is a service provider in Washington and Alaska to BCBS plans across the country.

What is Premera doing to protect you?

We recognize this issue can be frustrating and we are taking steps to protect you. We are providing protection and assistance to those affected by this cyberattack, including two years of free credit monitoring and identity theft protection services.

Specifically, we are providing you a **free, two-year membership in Experian's® ProtectMyID® Alert** to help detect possible misuse of your personal information and provide you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. Due to privacy laws, we are not able to enroll you directly. **For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your free, two-year membership, please see the additional information provided in this letter.**

We also recommend that you regularly review the Explanation of Benefits (EOB) statements your health insurer sends you. If you identify medical services listed on your EOB that you did not receive, please contact your health insurer immediately.

What has Premera done to prevent this from happening in the future?


Along with steps we took to cleanse our IT system of issues raised by this cyberattack, Premera is taking additional actions to strengthen and enhance the security of our IT systems moving forward.

Where can you get more information on this issue?

You have two options to obtain more information, online or via phone. You can visit <http://www.premeraupdate.com> for more information. Or, call 1-800-768-5817, Monday through Friday, 5:00 a.m. to 8:00 p.m. Pacific Time (closed on U.S. observed holidays). TTY/TDD users should call 1-877-283-6562.

I want you to know that protecting your information is incredibly important to us at Premera, as is helping you through this situation with the information and support you need.

Sincerely,

A handwritten signature in black ink, appearing to read "Jeffrey Roe", written in a cursive style.

Jeffrey Roe
President & CEO

Activate ProtectMyID Now in Two Easy Steps

1. ENSURE **That You Enroll By: September 30, 2015** (You will not be able to enroll after this date.)
2. VISIT the **ProtectMyID Web Site: www.protectmyid.com/premera**

If you have questions related to the product being offered or need an alternative to enrolling online, please call 888-451-6558 and provide engagement #: **PC92585**.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report:** See what addresses, employers, public records and accounts are already associated with you.
- **Alerts for:**
 - **3-Bureau Credit Monitoring:** Alerts you of new accounts appearing on your Experian, Equifax® and TransUnion® credit reports.
 - **3-Bureau Active Fraud Surveillance:** Daily monitoring of 50 potential indicators of fraud appearing on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
 - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 888-451-6558.

INFORMATION ABOUT PREVENTING IDENTITY THEFT

Even if you choose not to take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax
PO Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-525-6285

Experian
PO Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
PO Box 2000
Chester, PA 19022
www.transunion.com
1-800-680-7289

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

*Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
1-877-438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.



BLUE CROSS

An Independent Licensee of the Blue Cross Blue Shield Association

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
Parent or Guardian of Member
<<First Name>> <<Last Name>>
<<Street Address>>
<<City>>, <<State>> <<Zip Code>>

<<Date>>

Dear Parent or Guardian of <<FirstName>> <<LastName>>:

I am writing to inform you that Premera Blue Cross ("Premera") was the target of a sophisticated cyberattack, and that some of your child's personal information may have been accessed by the attackers. As part of our investigation, we notified the FBI and are coordinating with their own investigation into this attack.

We at Premera take this issue seriously and regret the concern it may cause. I'm writing to provide you information on the steps we are taking to protect you and your child's information moving forward.

What happened?

On January 29, 2015, we discovered that cyberattackers had executed a sophisticated attack to gain unauthorized access to our Information Technology (IT) systems. Our investigation further revealed that the initial attack occurred on May 5, 2014. We worked closely with Mandiant, one of the world's leading cybersecurity firms, to conduct our investigation and to remove the infection created by the attack on our IT systems.

Our investigation determined that the attackers may have gained unauthorized access to your child's information, which could include your child's name, address, telephone number, date of birth, member identification number, Social Security number if it is part of your child's member identification number or patient identifier, email address if provided to us, and claims information, including clinical information. 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.

Why does Premera have your child's information?

We believe your child has or had health plan coverage through another independent Blue Cross Blue Shield (BCBS) plan, and that your child may have received services in Washington or Alaska at some point since 2002. Premera is a service provider in Washington and Alaska to BCBS plans across the country.

What is Premera doing to protect you?

We recognize this issue can be frustrating and we are taking steps to protect you and your child. We are providing protection and assistance to those affected by this cyberattack, including two years of free credit monitoring and identity theft protection services.

Specifically, we are offering you a **free two-year membership in Family Secure® from Experian®**. Family Secure monitors your Experian credit report to notify you of key changes. In addition, Family Secure will tell you if your minor has a credit report, a potential sign that his or her identity has been stolen. Family Secure is completely free and will not hurt your credit score. **For more information about Family Secure and instructions on how to activate the complimentary two-year membership, please see the additional information provided in this letter.**

We also recommend that you regularly review the Explanation of Benefits (EOB) statements your health insurer sends your child. If you identify medical services listed on your child's EOB that your child did not receive, please contact your health insurer immediately.

What has Premera done to prevent this from happening in the future?

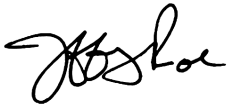
Along with steps we took to cleanse our IT system of issues raised by this cyberattack, Premera is taking additional actions to strengthen and enhance the security of our IT systems moving forward.

Where can you get more information on this issue?

You have two options to obtain more information, online or via phone. You can visit <http://www.premeraupdate.com> for more information. Or, call 1-800-768-5817, Monday through Friday, 5:00 a.m. to 8:00 p.m. Pacific Time (closed on U.S. observed holidays). TTY/TDD users should call 1-877-283-6562.

I want you to know that protecting your information is incredibly important to us at Premera, as is helping you through this situation with the information and support you need.

Sincerely,

A handwritten signature in black ink, appearing to read "Jeffrey Roe", written in a cursive style.

Jeffrey Roe
President & CEO

To receive the complimentary Family Secure product, you as the parent or guardian of the minor must enroll at the web site below.

Activate Family Secure Now in Two Easy Steps

1. **ENSURE That You Enroll By: September 30, 2015** (You will not be able to enroll after this date.)
2. **VISIT the Family Secure Web Site to enroll:** <http://www.familysecure.com/premera>

If you have questions related to the product being offered or need an alternative to enrolling online, please call 888-451-6558 and provide engagement #: **PC92586**

What features does your 24-MONTH Family Secure membership include once activated?

Parent or Legal Guardian:

- Daily monitoring of your Experian credit report with email notification of key changes, as well as monthly “no-hit” reports
- 24/7 credit report access: Unlimited, on-demand Experian reports and scores
- Experian credit score illustrator to show monthly score trending and analysis

Children:

- Monthly monitoring to determine whether enrolled minors in your household have an Experian credit report
- Alerts of key changes to your children’s Experian credit report

All Members:

- Identity Theft Resolution assistance: Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies
- \$2,000,000 Product Guarantee*

Once your enrollment in Family Secure is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about Family Secure, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian’s customer care team at 888-451-6558.

INFORMATION ABOUT PREVENTING IDENTITY THEFT

In addition, we recommend that you remain vigilant to the possibility of fraud and identity theft over the next 12 to 24 months by reviewing your child’s account statements and immediately reporting any suspicious activity to us. You may also obtain a copy of your child’s credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your child’s credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You should periodically obtain credit reports from each of the nationwide credit reporting agencies and request that any fraudulent activity be deleted. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax
PO Box 740241
Atlanta, GA 30374
www.equifax.com
1-800-525-6285

Experian
PO Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
PO Box 2000
Chester, PA 19022
www.transunion.com
1-800-680-7289

If you believe you or your child is the victim of identity theft or have reason to believe your or your child’s personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. Contact information for the Federal Trade Commission is as follows:

*The Family Secure Product Guarantee is not available for Individuals who are residents of the state of New York.

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
1-877-438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your or your child's records.

April XX, 2015

[Former ASO Group Policymaker Name]
Former ASO Group Policymaker Title]
[Former ASO Group Name]
[Street Address]
[City], [State] [Zip]

Re: Premera Breach Notification

Dear [Former ASO Customer],

On March 17, 2015, Premera Blue Cross announced that the company was the victim of a cyber-attack during which attackers gained unauthorized access to Premera's information technology system. The attack was discovered on January 29, 2015 and the subsequent investigation revealed that the initial attack occurred on May 5, 2014. Premera delayed notification about this attack based on strong advice that Premera first block the attack and cleanse their IT system before any public notification to prevent any additional malicious activity or any greater risk to affected members.

Premera notified the FBI and is fully cooperating with the Bureau's investigation into this attack. Premera 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. Premera continues to work with Mandiant to further strengthen the security of Premera's systems.

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

The Premera attack involved the information of members of other BlueCross and BlueShield plans who live in and/or sought treatment in Premera's service area, which includes Alaska and Washington State. That is because 37 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 lived in and/or received health care services in Premera's service area in Alaska and Washington State since 2002, their information should not be at risk. More information about this incident can be found at www.premeraupdate.com.

Affected Plan Members

Findings from Premera's investigation into the attack have identified members in your group health plan, which was previously administered by Capital BlueCross, whose information was accessed. According to Premera, the information accessed may have included name, date of birth, address, telephone number, email address, Social Security number, member identification number, and claims information, including clinical information.

A list of the names of your group's affected members is available upon request. To obtain the list, please send a letter requesting this information on your company letterhead to:

*Privacy Office
Capital BlueCross
P.O. Box 772132
Harrisburg, PA 17177-2132*

Notification by Mail to Affected Members

During the next several weeks, Premera is sending notification by U.S. mail to your members whose information was accessed. Each affected member will be provided with two years of free credit monitoring and identity theft protection services.

There are two versions of Premera's notification to affected members- one for adults and one for minors under the age of 18 at the time of the mailing. Copies of both notifications are enclosed.

Important notes concerning our letter to you and Premera's notification to affected members:

- If another BlueCross BlueShield system plan has served as your plan administrator at any time since 2002, you may receive a letter from that plan in addition to this letter. However, affected members will only receive one notification from Premera.
- You may have members who receive a Premera notification who were not covered by your ASO group plan previously administered by Capital BlueCross. This may be because those individuals were enrolled in another plan at some point since 2002 that was administered by another BlueCross BlueShield system plan, such as one offered through a different employer.

HITECH Breach Notification and HHS

Premera 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. Premera's notification to HHS will cover all affected BlueCross BlueShield system plans and their self-funded group health plans, so there is no need for your plan to make a separate notification to HHS.

Identity Protection Services for Members

Premera is working with Experian, a leading identity protection provider, to offer two years of free identity theft repair and credit monitoring services to all current and former BlueCross and BlueShield plan members whose information was affected. Any affected adult member will be offered Experian's ProtectMyID Alert and any affected minor member under the age of 18 will be offered Experian's FamilySecure. Any individual who believes they may have been affected by this attack and wants to enroll in these services prior to receiving their letter, may do so by following the instructions for enrollment found at: www.premeraupdate.com.

Toll-Free Hotline for Members

Premera has established a dedicated toll-free number that members can call if they have questions related to this incident. The number is 1.800.768.5817 and it is open Monday through Friday, between 8:00 a.m. and 11:00 p.m. Eastern Daylight Time.

Additionally, consumers may contact the Pennsylvania Attorney General's Health Care Section Helpline at 1.877.888.4877 or 717.705.6938 for further assistance.

Capital BlueCross' Commitment to Information Security

Again, Capital BlueCross systems were not impacted by, and were not part of, the attack on Premera.

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.

We are Here to Answer Your Questions

We understand that the Premera attack and the information shared in this letter may cause concern and generate questions – and we are here to help. If you have questions, please contact us at 1.866.814.7544.

We will provide you with responses as quickly as possible.

Sincerely,

Tracy Onorofsky
Senior Vice President, Commercial Group Sales