Answers to Your Questions About the Cyber-Attack on Premera Blue Cross

What is the situation?

On March 17, 2015, Premera Blue Cross announced that it had been the target of a sophisticated cyber-attack through which attackers gained unauthorized access to Premera’s information technology system. Premera operates Blue Cross and Blue Shield plans in Washington state and Alaska, but not in Florida.

Premera has said that it discovered the attack on January 29, 2015 and an investigation further revealed that the initial attack occurred on May 5, 2014. Premera reported that the attackers may have gained access to personal information of current and former members dating back to 2002. In addition, information pertaining to some current or former members of other independent Blue Cross and Blue Shield plans, including Florida Blue, could have been accessed by the cyber-attackers.

Some Florida Blue members could have been impacted if they lived in and/or received medical services in Washington state or Alaska at some point since 2002. This is because, through certain collaborative arrangements such as the BlueCard program, Premera acts as a service provider in Washington and Alaska for other plans, including Florida Blue.

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

Premera immediately engaged the FBI and Mandiant, a leading cybersecurity firm also used by Anthem in response to the cyber-attack it experienced. Premera delayed its notification until March 17 based on strong advice from these experts that it should block the attack and cleanse its IT systems before making a public announcement. Premera was 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 disclosed the attack before finishing its investigation and enhancing its IT security.

Is this incident related to the cyber-attack on Anthem?

Both attacks are the subject of active FBI investigations. Apart from that, we are not in a position to comment knowledgeably about any connection.

What is the connection between Anthem and Premera?

Premera and Anthem are both part of the Blue Cross and Blue Shield system, as is Florida Blue. The system includes 37 independent, locally operated companies across the U.S. This affiliation (or system) enables Blue Cross and Blue Shield members to access high-quality health care anywhere in the country.
What kind of information did the cyber-attackers access?

According to Premera, the information the cyber-attackers accessed may have included current and former members’ names, birth dates, medical IDs, addresses, email addresses, telephone numbers, social security numbers, and claims information, including clinical data. Premera has said that there is no evidence that the information was removed from the information technology system or that it has been used inappropriately.

How is the attack on Premera similar to or different from the recent cyber-attack on Anthem?

Both cyber-attacks are the subject of active investigations by the FBI. Premera operates in fewer states than Anthem and fewer individuals’ information was accessed. The data accessed in the attack on Premera included claims information, including clinical data. But, unlike Anthem’s cyber-attack, Premera has said that there is no evidence that the information was removed from the information technology system.

Did the cyber-attackers access personal information of Florida Blue members?

We are actively engaged with Premera to determine who among our members might have been impacted. Florida Blue members could have been impacted if they lived in and/or received medical services in Washington state or Alaska at some point since 2002. This is because, through certain collaborative arrangements such as the BlueCard program, Premera acts as a service provider in Washington and Alaska for other plans, including Florida.

How will I know if my personal information has been accessed? When will I hear?

We are committed to helping Florida Blue members understand whether they were affected by the cyber-attack on Premera and what resources are available to them. We will be reaching out to impacted members via mail in the next few weeks, as will Premera. Premera is providing two years of free credit monitoring and identity theft protection services to those individuals. Premera has also established a dedicated call center for affected individuals. More information can be found at PremeraUpdate.com.

How soon can members access credit monitoring services?

We recognize that members may be anxious to enroll in credit monitoring and identity theft repair services prior to receiving notification that they have been impacted. As such, Premera is offering access to these services now. Further information about enrolling is available at PremeraUpdate.com.

What else can I do to protect my identity?

Anyone who may have been impacted by the cyber-attack against Premera should be vigilant and look for signs that someone has stolen their personal information and is using it without their permission. Steps you can take right now include carefully reviewing account statements and ordering free credit
How will I know if my health insurance identification number has been compromised? Is there anything that I can do to monitor this?

If you have signed up for Florida Blue’s member portal, you can check claim activity by logging into your account at [www.FloridaBlue.com](http://www.FloridaBlue.com). If you have not already registered for Florida Blue’s member portal, you can create an account by accessing [www.FloridaBlue.com](http://www.FloridaBlue.com) from your mobile device or computer. If you use your mobile device, select the green button that says “member login.” If you use your computer, select the blue button that says “login/register.” You will need your member number in order to register.

You also should carefully review any paper correspondence (e.g., explanations of benefits, invoices) you receive from your providers or Florida Blue.

What is Florida Blue doing to protect my personal information?

Protecting our members’ personal information is of utmost importance to us. Florida Blue members who were impacted by the Premera cyber-attack will receive a letter from Florida Blue in the mail as well as an official notification letter from Premera. Premera’s notification letter will be mailed in an envelope branded Premera Blue Cross.

Our Information Security team is constantly implementing tools and processes to prevent security breaches such as this. Florida Blue employs a data security framework that is designed to protect our members’ information against unauthorized access and is committed to evaluating and enhancing its data security practices, as needed, to ensure that they meet or exceed standard for the industry. It is standard business practice and a company priority to take appropriate steps to minimize the risk of members’ personal information being compromised as a result of a cyber-attack.

What actions has Florida Blue taken in response to recent cyber-attacks on other plans?

Our security policies and protocols have been built to provide rigorous data protection and are designed with an understanding that our efforts must be aimed at preventing, detecting, containing and correcting any potential security threats.

Data security starts by managing the data from its inception. Every Blue Cross and Blue Shield company gathers and shares only the minimum amount of customer information needed to efficiently manage the processes that allow us to help ensure that health care professionals have the information, resources and tools they need to provide quality patient care.
In the normal course of business, our Information Security group constantly monitors our systems to guard against cyber-attacks. Nonetheless, in light of recent attacks, we are conducting additional security reviews and so far have found no evidence that our information system was compromised.

**What is the Blue Cross Blue Shield system as a whole doing about cybersecurity?**

Collectively, Blue Cross and Blue Shield companies are committed to doing everything we can to ensure the security and privacy of customers against those who are intent on stealing personal information. Staying ahead of these very serious threats has been, and will continue to be, a top priority for the Blue Cross Blue Shield system.

Blue Cross and Blue Shield companies use a combination of internal and externally contracted persistent defenses to ensure that we are mitigating potential threats and that we have strong privacy and data protection capabilities in place. All plans have implemented multiple controls and protections that are used to keep sensitive and confidential information secure.