What is the situation?

Anthem, Inc. experienced an external cyber-attack that was first reported in the media on Wednesday, Feb. 4, 2015. Anthem is an Indianapolis-based company that operates Blue Cross and Blue Shield plans in 14 states, but not in Florida.

Anthem reported that hackers obtained unauthorized access to a database containing personal information on its current and former members and employees dating back to 2004. In addition, Anthem reported that this database also contained personal information on some members whose medical claims were processed by Anthem over this same time period, as a result of their having received health care services in the Anthem service areas.

What kind of information did the cyber-attackers access?

According to Anthem, the information hackers accessed may have included current and former members’ names, birth dates, medical IDs, street addresses, email addresses, telephone numbers and social security numbers. Anthem reported that it had no evidence that the hackers were able to access any medical or credit card information.

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

Yes. According to our analysis of the data Anthem provided to us, some Florida Blue members were impacted by the cyber-attack. These members were affected because they received care while living or traveling in Anthem’s 14-state service area during the last 10 years. This is because, through an arrangement known as the BlueCard program, Anthem may have processed our members’ claims for medical services.

My children are on my insurance plan. Was their information also accessed?

Based on our analysis of the data that Anthem provided to us, both adults and children were impacted by the cyber-attack.

In what states does Anthem operate Blue Cross and Blue Shield plans?

Anthem operates plans in California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia and Wisconsin.
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 Anthem and what resources are available to them. To ensure our members receive the most timely notice possible, Florida Blue is reaching out to impacted members via mail in advance of a separate, official notification that they will receive from Anthem. Individuals will begin to receive letters in the coming weeks.

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, Anthem is offering access to these services now.

The free identity protection services offered by Anthem include two years of:

- Identity repair assistance
- Credit monitoring
- Child identity protection
- Identity theft insurance
- Identity theft monitoring/fraud detection
- Phone alerts

Further information about enrolling is available on the Internet at AnthemFacts.com and via telephone at 877-263-7995. Spanish speaking members may access information at AnthemInforma.com or receive assistance in Spanish at 877-263-7995.

What else can I do to protect my identity?

Anyone who may have been impacted by the cyber-attack against Anthem 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 reports. In addition, you can report suspected incidents of identity theft to local law enforcement, Federal Trade Commission, or your state’s attorney general. To learn more, you can go to the FTC’s Web site, at www.consumer.gov/idtheft, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You should be aware of scam email campaigns targeting current and former Anthem members. These scams, designed to capture personal information (known as “phishing”), are designed to appear as if they are from Anthem and the emails include a “click here” link for credit monitoring. These emails are NOT from Anthem.

- DO NOT reply to the email or reach out to the senders in any way.
- DO NOT supply any information on the website that may open, if you have clicked on a link in email.
• DO NOT open any attachments that arrive with email.

Neither Anthem nor Florida Blue is calling members regarding the cyber-attack or asking for credit card information or social security numbers over the telephone. However, when you enroll in the identity theft repair and credit monitoring services you may be asked to provide your social security number.

**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 Anthem cyber-attack will receive a letter from Florida Blue in the mail in advance of an official notification letter from Anthem. Anthem’s notification letter will be mailed in an envelope branded Anthem, Inc.

Additionally, 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 are industry standard. It is standard business practice and a company priority to take all 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 the attack on Anthem?**

In the normal course of business, our Information Security group constantly monitors our systems to guard against cyber-attacks. Nonetheless, in light of the cyber-attack on Anthem, we recently conducted a thorough security review and found no evidence that our information system was compromised.