JOINT INDUSTRY BOARD OF THE ELECTRICAL INDUSTRY
158-11 HARRY VAN ARSDALE JR. AVENUE • FLUSHING, N.Y. 11365
TEL: (718) 591-2000 • FAX: (718) 380-7741 • www.jibei.org

February 2015

IMPORTANT INFORMATION

FOR ALL PARTICPANTS IN THE DENTAL BENFIT PLAN OF THE ELECTRICAL INDUSTRY AND THE DENTAL BENEFIT PLAN OF THE ELEVATOR INDUSTRY

As you have probably heard on the news, Anthem, the parent company of Empire Blue Cross was the target of a very sophisticated external cyber-attack. Empire Blue Cross is the administrator of our Dental Plans. At the present time we do not know if our dental participants were subject to this cyber-attack. These attackers gained unauthorized access to Anthem's IT system and have obtained personal information from current and former participants such as their names, birthdays, medical IDs/social security numbers, street addresses, email addresses and employment information, including income data. Based on what we know now, there is no evidence that credit card or medical information, such as claims, test results or diagnostic codes were targeted or compromised.

Once the attack was discovered, Anthem immediately made every effort to close the security vulnerability, contacted the FBI and began fully cooperating with their investigation.

You will be receiving a letter from Anthem through the U.S. Postal Service if your information was compromised. Scammers have already tried contacting people by email claiming to be Anthem Blue Cross in an attempt to obtain your information. You are advised **NOT** to open any email alleging it is from Anthem or Empire.

Anthem will provide credit monitoring and identity protection services free of charge so that those who have been affected can have peace of mind. The Company has created a dedicated website www.AnthemFacts.com where participants can access information such as frequently asked questions and answers. Anthem has also established a dedicated toll-free number you can call for information **1-877-263-7995**. As Anthem learns more, they will continually update this website and share that information with you.

Enclosed is an informative press release from Empire Blue Cross and an article that appeared in the New York Times. The Joint Industry Board does not currently have any additional information regarding this incident and its effect on Participants in our Dental Plans. Empire Blue Cross does not administer our major medical or hospitalization plan, nor do they have access to those records.

Please check our website www.jibei.org for updates.

The Joint Industry Board of the Electrical Industry will closely monitor this situation and will make sure that the participants of our Dental Plans are informed regarding this incident.

Press Release

Empire BlueCross BlueShield Alerts Consumers to Protect Themselves from Scam Email Campaigns

Media Contact: Sally Kweskin, 212-476-1421, sally.kweskin@empireblue.com**, @empirebcbs**

NEW YORK, NY, February 6, 2015 — New York residents who may have been impacted by the cyber attack against Anthem, should be aware of scam email campaigns targeting current and former Empire BlueCross BlueShield and Empire BlueCross members. These scams, designed to capture personal information (known as "phishing") are designed to appear as if they are from Anthem, (Empire's parent company), and the emails include a "click here" link for credit monitoring. These emails are NOT from Anthem or Empire.

- DO NOT click on any links in email.
- 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.

Empire also is NOT calling members regarding the cyber attack and is not asking for credit card information or social security numbers over the phone.

This outreach is from scam artists who are trying to trick consumers into sharing personal data. There is no indication that the scam email campaigns are being conducted by those that committed the cyber attack, or that the information accessed in the attack is being used by the scammers.

Empire will contact current and former members via mail delivered by the U.S. Postal Service about the cyber attack with specific information on how to enroll in credit monitoring. Affected members will receive free credit monitoring and ID protection services.

For more guidance on recognizing scam email, please visit the FTC Website: http://www.consumer.ftc.gov/articles/0003-phishing. Additional information about the cyber attack against Anthem is available at www.AnthemFacts.com.

About Empire BlueCross BlueShield

Serving New Yorkers for 80 years, Empire BlueCross BlueShield is the largest health insurer in New York supporting nearly five million members and more than 38,000 business, union and small employers in New York. Empire BlueCross BlueShield (Empire) is the trade name of Empire HealthChoice Assurance, Inc., and Empire Blue Cross Blue Shield HMO is the trade name of Empire HealthChoice HMO, Inc., independent licensees of the Blue Cross Blue Shield Association, serving residents and businesses in the 28 eastern and southeastern counties of New York State. Additional information about Empire is available at www.empireblue.com. Also, follow us on Twitter at www.twitter.com/healthjoinin or @empirebcbs, on Facebook at www.facebook.com/HealthJoinIn, or visit our YouTube channel at www.youtube.com/healthjoinin

The New York Times | http://nyti.ms/1zgNTMV

YOUR MONEY

What Anthem Customers Should Do Next After Data Breach

By TARA SIEGEL BERNARD FEB. 6, 2015

Consumers' first worry in a major security breach is usually about their financial and credit accounts. But cyberthieves can do some serious damage with medical information as well.

Anthem Health said this week that hackers obtained names, addresses, Social Security numbers, birthdays, email and employment information on up to 80 million current and former customers and Anthem employees. Although Anthem says the attackers did not get any medical records, they did get access to medical identification numbers found on insurance cards. Anthem offers several Blue Cross and Blue Shield insurance plans across the country.

"You don't need a complete medical record to commit medical identity theft if you have the correct name and Social Security number," said Pam Dixon, executive director of World Privacy Forum. "The chief harm for medical identity theft is that your medical record will change without your knowledge."

And in this case, the hackers have enough information to do exactly that. Here's what you need to know:

THEFT TYPES In large-scale breaches like the one at Anthem, experts said the criminals could pose as medical billers and fraudulently charge consumers' insurance companies for medical services and drugs. Not only is your insurer paying for something that you didn't ask for, but the fraudsters can also alter your medical record, Ms. Dixon said.

With an insurance ID number in hand, it can be easier for criminals to

attempt to acquire medical records or insurance codes to help guide them on what to bill for, she explained. “Searches through the data for cancer survivors or even those in current cancer treatment would allow for fake billing to be piggybacked onto the real billing. This makes it extremely difficult for the health plan to detect the fake billing, and the thieves then will get a stream of payouts over time. It adds up to a lot of money quickly.”

Anthem has said that it does not believe medical information like insurance claims or test results were compromised. Hospital and doctor information is also believed to have been spared.

WHAT TO DO Consumers should try to create their own copy of their medical file so they have an accurate version of their history should a fraudster make any changes, said Ms. Dixon, who has worked with many medical identity theft victims. Think about any significant or chronic medical conditions, surgeries or accidents — particularly for the last few years — and get a record from your doctors’ offices, hospital or other provider. Also get a record of your blood type and any drug allergies. If you have access to an online patient portal, try to print out or save a copy of those files elsewhere.

“You want to print a baseline record so that if it is altered without your knowledge by fraudulent activity,” Ms. Dixon said, “you have something that is really clean.” That will help prove your case, she said, and rebuild an accurate history.

WHAT TO MONITOR If you have online access to any of your medical records through a patient portal, keep a watchful eye for any suspicious activity. And closely monitor your explanation of benefit statements to be sure they do not include any services you did not receive (and if you suspect you are not receiving your statements, report that to your insurer as well). Credit-monitoring services may help pick up medical debt collections in your name that you do not owe, and calls from collectors may be another warning signal.

Also remember this is a long-term crime. Fraudulent activity may not show up for six months to a year, experts said, so a heightened sense of awareness and vigilance needs to become routine.

WHAT’S HAPPENING NOW Scam artists have already started sending emails that appear to be from Anthem’s insurers in an attempt to trick people into sharing personal data. The company said there was no indication that the scams were being conducted by the same thieves who conducted the cyberattack.

Anthem said it would contact current and former members via mail delivered by the United States Postal Service about the breach with specifics on how to enroll in free credit monitoring and ID protection services, which will be provided for a year. It cautioned not to click on any links in emails that appear to be from the company, and said not to open attachments, reply to senders or supply any information.

Anthem created a website, www.AnthemFacts.com, and a toll-free number, 1-877-263-7995, to respond to questions.
