STATE OF WISCONSIN
Department of Employee Trust Funds
Robert J. Conlin
SECRETARY

801 W Badger Road
PO Box 7931
Madison WI 53707-7931

1-877-533-5020 (toll free)
Fax 608-267-4549
etf.wi.gov

TO: **Employers Participating in the State of Wisconsin Group Health Insurance Program**

FROM: **Wisconsin Department of Employee Trust Funds**

RE: **Anthem database breach – Talking Points and Frequently Asked Questions**

DATE: **February 6, 2015**

The following will help you communicate to your employees about the Anthem Blue Cross Blue Shield database breach, reported earlier this week. The bullet points are "talking points" for your use and/or dissemination, as is the list of Frequently Asked Questions and Answers.

Talking Points

- Health insurer Anthem Blue Cross Blue Shield (Anthem) was recently the target of a sophisticated external cyber attack.

- These cyber attackers gained unauthorized access to information technology system databases containing personal information of current and former Anthem *members.*

- The Anthem data breach may affect current and former members and dependents who have health coverage and dental coverage through the following plans currently or previously offered by the State of Wisconsin Group Health Insurance Program:
  - Anthem Blue Preferred-Southeast Network
  - Anthem Blue Preferred-Northeast Network
  - Anthem Blue Preferred-Northwest Network (offered through 2013)
  - Anthem Dental Blue
  - Standard Plan (1994 – 2005)

- The Department of Employee Trust Funds, administrator of the State of Wisconsin Group Health Insurance Program, has posted a communication to members about this event on its website.

- The type of information accessed includes member names, birth dates, member health ID numbers, Social Security numbers, mailing and email addresses, and

employment information. Thus far, Anthem officials believe that specific medical information and credit card numbers were neither targeted nor compromised.

- Anthem will contact current and former members whose information has been accessed with detailed information and instructions. In the meantime, more information is available at www.AnthemFacts.com or by calling Anthem toll free at 1-877-263-7995.

- Anthem has contacted the Federal Bureau of Investigation and has also retained a cybersecurity firm to provide incident response and security assessment services.

- Anthem is not aware of any fraud that has occurred as a result of this incident against its members, but all affected members will be enrolled in identity repair services. In addition, impacted members will be provided information on how to enroll in free credit monitoring.

- This type of event would not be considered a reason for individual members to cancel enrollment in Anthem.

Anthem Blue Cross Blue Shield
Answers to Employee Frequently Asked Questions

Was my information accessed?
Anthem is currently conducting an extensive investigation to determine what members – current as well as former -- are affected. Anthem members who are affected will be contacted by Anthem.

What information was compromised?
Anthem's initial investigation indicates that the member data accessed included names, dates of birth, member health ID numbers/Social Security numbers, addresses, telephone numbers, email addresses and employment information including income data.

Was there any diagnosis or treatment data exposed?
Anthem's investigation to date indicates there is no evidence that medical information, such as claims, test results, or diagnostic codes were targeted or compromised.

Was my credit card information accessed?
Anthem's investigation to date indicates there is no evidence that credit card information was compromised.

Do the people who accessed my information have my Social Security number?
Anthem's investigation to date indicates that the information accessed included names, dates of birth, member health ID numbers/Social Security numbers, street addresses, email addresses and employment information. Anthem is working to determine whose Social Security numbers were accessed.

How can I sign up for credit monitoring services?

All affected members will receive notice, via mail, which will advise them of the protections being offered to them as well as any next steps.

When will I receive my letter in the mail?
We continue working to identify the members who are affected and expect the mailing of letters to begin in the next two weeks.

My children are on my insurance plan; was their information also accessed?
Anthem is currently conducting an extensive investigation to determine which members are affected. Anthem's investigation to date indicates adults and children were affected.

Do the people who accessed my information know about my medical history?
Our investigation to date indicates there was no diagnosis or treatment data exposed.

Do the people who accessed my information have my credit card numbers and banking information?
No, the investigation to date indicates that information accessed did not include credit card numbers, banking or other financial information.

Has anyone used my information yet?
We are not aware of any fraud that has occurred as a result of this incident against our members.

Am I at risk for identity theft?
Anthem is currently conducting an extensive investigation to determine which members are affected. We are not aware of any fraud that has occurred as a result of this incident against our members, but all affected members will be enrolled in identity repair services. In addition, affected members will be provided information on how to enroll in free credit monitoring.

Do I need a new member ID card and number?
Anthem is working around the clock to determine how many people have been affected and will notify all who are affected. Anthem will provide further guidance on next steps.

How can I be sure my personal and health information is safe with Anthem, Inc.?
Safeguarding its members' personal, financial and medical information is a top priority for Anthem, and because of that, they have a state-of-the-art information security system to protect the data. Anthem has contracted with Mandiant, a global company specializing in the investigation and resolution of cyber attacks. Anthem will work with Mandiant to ensure there are no further vulnerabilities and work to strengthen security.

What is Anthem doing to help members potentially affected by this incident?
All affected members will be enrolled in identity repair services. In addition, affected members will be provided information on how to enroll in free credit monitoring.

Where is the data now? And who can access my information?
Evidence indicates the data was uploaded to an external file sharing service. This file sharing service, at Anthem's request, has locked down the account and data so that it cannot be copied, accessed or removed. Anthem and the FBI are working with the file sharing service to access the data and further secure it.