URGENT NOTICE – ANTHEM CYBER ATTACK – DATA BREACH

It was brought to our attention on February 5, 2015, that Anthem, Inc., the parent company of Anthem Blue Cross, is the victim of a highly-sophisticated cyber attack. Anthem has informed their TPA's. which have notified us, that its member data was accessed, and information about our clients could be among the data.

Our TPA's are working closely with Anthem to better understand the impact on its members. They are in turn notifying brokers about the situation as it becomes available.

Here is what we do know:

- Once Anthem determined it was the victim of a sophisticated cyber attack, it immediately notified federal law enforcement officials and shared the indicators of compromise with the HITRUST C3 (Cyber Threat Intelligence and Incident Coordination Center).
- Anthem's Information Security has worked to eliminate any further vulnerability and continues to secure all of its data.
- Anthem immediately began a forensic Information Technology (IT) investigation to determine the number of impacted consumers and to identify the type of information accessed. The investigation is still taking place.
- The information accessed includes member names, member health ID numbers/Social Security numbers, dates of birth, addresses, phone numbers, email addresses and employment information, including income data. Social Security numbers were included in only a subset of the universe of consumers that were impacted.
- Anthem is still working to determine which members' Social Security numbers were accessed.
- Anthem's investigation to date shows that no credit card or confidential health information was accessed.
- Anthem has advised us there is no indication at this time that any of our clients' personal information has been misused.
- All impacted Anthem members will be enrolled in identity repair services. In addition, impacted members will be provided information on how to enroll in free credit monitoring.

We are continuing to work closely with Anthem to better understand the cyber attack and the impact on our clients. Anthem has created a website-www.anthemfacts.com, and a hotline, 1-877-263-7995 for its members to call for more information, and has shared the attached FAQ that further explains the cyber attack.

We will continue to keep you updated on Anthem's ongoing investigation in hopes to find out who committed the attack, and why.

Below is the formal breach notification and assessment, as well as attachments provided by Anthem for review.

Breach Notification

- **Disclosure Tracking Number:** 201501309249

- **Date we discovered the disclosure:** 01/29/15

- **Date of the Disclosure:** Query activity started on December 10, 2014 and continued sporadically until January 27, 2015.

- **How was disclosure discovered:** On January 27, 2015, an Anthem associate, a database administrator, discovered suspicious activity - a data query running using the associate's logon information. He had not initiated the query and immediately stopped the query and alerted Anthem's Information Security department. It was discovered that logon information for additional database administrators had been compromised.

  On Jan. 29, 2015, we determined that we were the victim of a sophisticated cyber attack. We notified federal law enforcement officials and shared the indicators of compromise with the HITRUST C3 (Cyber Threat Intelligence and Incident Coordination Center).

- **Member(s) Impacted:** TBD

- **Type of PHI (be very specific and include all):** Initial investigation indicates that the member data accessed included names, member ID numbers, dates of birth, social security numbers, addresses, phone numbers, email addresses and employment information including income data. Our investigation to date shows there was no credit card or debit card information or medical health treatment information compromised.

- **Type of Incident:**The attack that occurred was highly sophisticated in nature and is what is called an APT - Advanced Persistent Threat. The attacker had a proficient understanding of the data platforms and successfully utilized valid database administrator logon information.

- **Where did incident take place:** N/A

- **Root Cause (must provide detailed descriptive):** TBD

Corrective Action:
Anthem has changed passwords and secured the compromised database warehouse. Additionally, 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. Additionally, Anthem will continue to work with the Federal Bureau of Investigations.

Has the impacted member been notified:
Written notification will be made to all impacted individuals with an offer of credit monitoring. In addition, all impacted individuals will be enrolled in a proactive identity repair

services. Required member notification under HITECH will be made where applicable. State law notice will be made through each state's "Substitute Notice" provision. We are not aware of any fraud that has occurred as a result of this incident against our members.