Update on Anthem Cyber Attack –

General Information for Clients and Brokers

February 20, 2015

What happened?

Anthem, Inc. was the victim of a cyber attack. Anthem discovered that one of its database warehouses was experiencing a suspicious data query. We immediately stopped the query and launched an internal investigation. Anthem took immediate action to secure its data and contacted federal investigators as soon as it made that discovery.

When and how did you discover the attack?

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

On January 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).

How many people are impacted?

Anthem is currently conducting an extensive IT Forensic Investigation to determine what members are impacted. We will provide additional details to our ASO clients as soon as it is available. Initial analysis indicates the attacker had access to information on tens of millions of consumers. This includes Anthem's affiliated health plan members and other consumers within the Blue Cross Blue Shield system. Social Security numbers were included in only a subset of the universe of consumers that were impacted.

Is there information Anthem clients and customers can provide to members who ask about the Anthem cyber attack?

Anthem encourages anyone with questions to go to **AnthemFacts.com** or call the toll-free number **1-877-263-7995**.

What information has been compromised?

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.

Was there any diagnosis or treatment data exposed?

No, we do not believe any diagnosis or treatment data was exposed.

Why should I trust you with my employee's data in the future?

Safeguarding our members' personal, financial and medical information is one of our top priorities, and because of that, we 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 measures have you taken to protect against further cyber attacks?

Anthem Information Security has been working to eliminate any further vulnerability and secure all its data. Cyber attacks are continually evolving and cyber attackers are becoming increasingly sophisticated. We are also working with federal law enforcement to attempt to ensure our environment is as secure as possible. Anthem's team of nearly 200 professionals has extensive technical and cyber security experience, and our Security Operations Center is staffed with a Detection Analysis and Response Team (DART) and a forensics lab that enables us to evaluate and thwart potential threats.

Security threats continue to evolve, raising the bar on the levels of security needed to respond to those threats. We continually assess our capabilities with third parties. We are HiTrust certified and have been considered an industry leader in many aspects of our security program.

As a result of the recent incident we are accelerating our efforts to introduce even more stringent security measures in 2015 to help ensure the security of our members' data. Our initiatives span several areas including:

- Implementing a complex, three tier multi-factor authentication process for all network and database administrator accounts.
- Enhancing and expanding our event logging capabilities for security and system logs.
- Enhancing security for end user convenience system access (Calendars, Contact Lists, Email) so that all access now requires two-factor authentication using a token.

- Enhancing our security monitoring capabilities by adding additional sensors and monitoring agents.
- Adding resources to our existing staff of 200.
- Investigating the use of encryption of data-at-rest for our existing databases.
- Expansion of existing DLP (Data Loss Prevention) technology.

What are your security protocols? Why didn't they work?

The attack that occurred was highly sophisticated in nature. The attacker had a proficient understanding of the data platforms. The attacker utilized very sophisticated tools and methods in which to carry out the attack and took care to cover tracks by moving from server to server within the environment, often using a different compromised user ID each time they connected to a different server.

The Anthem associate who discovered the suspicious query activity followed appropriate protocol and immediately notified Information Security. Anthem immediately launched an investigation. Once Anthem determined it was a cyber attack, Anthem contacted federal investigators.

Anthem has changed passwords and secured the compromised database warehouse.

Do you recommend members change their password on the secure member site?

While there is no evidence in our investigation to date to suggest that member information or credentials were compromised related to any of our Anthem websites, we always encourage our members and associates to frequently change personal passwords that are used to access sensitive data.

How will members be notified that their information was in the database?

We are working around the clock to identify the members whose information was accessed. This work takes time, and while we are working as fast as we can, we also want to ensure we correctly identify everyone who is impacted by this attack. This work is being conducted simultaneously with the FBI and Mandiant investigations into the cyber attack.

Will members receive a letter in the mail from Anthem?

Yes, Anthem will begin to mail letters to all impacted current and former members in the coming weeks. Those letters will provide information on free identity repair services and credit monitoring. However, members can access these services now — they do not have to wait until they receive notification from Anthem. A copy of the letter is posted on **AnthemFacts.com.**

Will Anthem send me an email with this information?

Members who have provided e-mail addresses to Anthem and have opted in to receiving communications may receive an e-mail directing them to visit **AnthemFacts.com** to sign up for credit protection services. This e-mail is scheduled to be distributed the week of February 16. The email will contain the exact same language of the mailed letter and is available on **AnthemFacts.com**.

This email is being sent due to state notification requirements. It will not ask for personal information and will not contain a link to any websites other than **AnthemFacts.com**.

If members receive any emails regarding the Anthem Cyber Attack asking for personal information, or asking them to click on an unfamiliar link:

- 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 an email.
- DO NOT open any attachments that arrive with email.

For more guidance on recognizing scam email, please visit the FTC website:

http://www.consumer.ftc.gov/articles/0003-phishing.

Is Anthem providing credit protection services?

Yes, Anthem is providing credit protection services, free of charge, for two years.

How can I enroll in credit protection services?

Identity theft repair services are available to Anthem members who feel they have experienced fraud. **For members who have been impacted by the cyber attack, these services are automatically available and do not require enrollment**. Please visit **AnthemFacts.com** to learn how to access these services. Members may also access identity repair services by calling **1-877-263-7995**.

Credit monitoring services require a member to actively enroll because the member must provide their personal information and consent to have their credit monitored. Members can enroll at any time during the 24 month coverage period, and can learn how to sign up at **AnthemFacts.com**. Members who do not have access to the Internet may call **1-877-263-7995** for assistance.

What times can I call to enroll in credit protection services?

Phone lines will be open from 2pm to 9 p.m. ET on Friday, February 13, and will be open 9 a.m. to 9 p.m. ET Monday to Saturday.

Spanish-speaking members may access information at **AnthemInforma.com**, or receive assistance in Spanish at **1-877-263-7995**.

What credit protection services is Anthem offering?

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

- *Identity Theft Repair Assistance*: Should a member experience fraud, an investigator will do the work to recover financial losses, restore the member's credit, and ensure the member's identity is returned to its proper condition. This assistance will cover any fraud that has occurred since the incident first began.
- *Credit Monitoring*: At no cost, members may also enroll in additional protections, including credit monitoring. Credit monitoring alerts consumers when banks and creditors use their identity to open new credit accounts.
- *Child Identity Protection*: Child-specific identity protection services will also be offered to any members with children insured through their Anthem plan.
- *Identity theft insurance*: For individuals who enroll, the company has arranged for $1,000,000 in identity theft insurance, where allowed by law.
- *Identity theft monitoring/fraud detection*: For members who enroll, data such as credit card numbers, Social Security numbers and emails will be scanned against aggregated data sources maintained by top security researchers that contain stolen and compromised individual data, in order to look for any indication that the members' data has been compromised.
- *Phone Alerts*: Individuals who register for this service and provide their contact information will receive an alert when there is a notification from a credit bureau, or when it appears from identity theft monitoring activities that the individual's identity may be compromised.

Why do members have to enroll in credit monitoring services?

Credit monitoring services require a member to actively enroll because the member must provide their personal information and consent to have their credit monitored. Members can enroll at any time during the 24 month coverage period, and can learn how to sign up at **AnthemFacts.com**. Members who do not have access to the Internet may call **1-877-263-7995** for assistance.

Are members at risk for identity theft?

Anthem is currently conducting an extensive IT Forensic Investigation to determine which members are impacted. We are not aware of any fraud that has occurred as a result of this incident against our members, but all impacted members will be eligible to receive identity repair assistance. Identity repair services provide affected customers with a dedicated investigator to assist them with fraud-related issues arising from this incident.

Do members need a new member ID card and number?

No, their current member ID card and number are valid and will provide them access to care.

Have all Anthem outbound calls stopped? People are very concerned all calls are fraud. Clinical, vendors, robo calls, etc.

No, we will continue to make outbound calls that are vital for our normal course of business, such as calls from our clinical staff to members who are enrolled in care management programs.

However, Anthem will not make outbound calls to members about the cyber attack, and will not ask members for their Social Security numbers, credit card or banking numbers with regard to the cyber attack.

Anthem 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 identity protection services.

For more guidance on recognizing scam email, please visit the FTC website:

http://www.consumer.ftc.gov/articles/0003-phishing.