Update on Anthem Cyber Attack —

General Information for Clients and Brokers

Empire BlueCross BlueShield

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 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).

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.

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 worked to eliminate any further vulnerability and continue to secure all its data. Cyber attacks are continually evolving and cyber attackers are becoming more sophisticated every day. We are also working with federal law enforcement to ensure our environment is as secure as possible.

Anthem continues to stay abreast of cyber attack methods and tools and works closely with many private and public organizations that specialize in the prevention, evaluation and investigations of cyber attacks.

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.

51797WPMENEBS 2/15

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.

Once we have identified all who are impacted, we will begin the process of distributing letters. We expect the mailing to begin in the coming weeks. We will share a more detailed communications timeline once impacted members have been identified.

Anthem will offer identity repair services, which will be retroactive to the date of the potential exposure, and credit monitoring, which is effective if and when the consumer enrolls, through a trusted vendor. We are in the final stages of preparation with the vendor, and anticipate members will be able to access the vendor hotline next week. At that time, members will be able to call the hotline and receive identity repair services, and if they chose, can also enroll in credit monitoring. Members will not need to wait until they receive their mailed notification. We will provide more detailed communications once the hotline is available.

We are notifying all impacted members by mail with an offer of free credit monitoring. We will also provide HITECH notice to those consumers affected where required by law. We will be making substitute notice under applicable state law through email, website notice, and media notice or as otherwise required under a state's breach notice provision for substitute notice. This includes current and prior members.

Can those impacted sign up for credit monitoring and repair services now?

Anthem will offer identity repair services, which will be retroactive to the date of the potential exposure, and credit monitoring, which is effective if and when the consumer enrolls, through a trusted vendor. We are in the final stages of preparation with the vendor, and anticipate members will be able to access the vendor hotline next week. At that time, members will be able to call the hotline and receive identity repair services, and if they chose, can also enroll in credit monitoring. Members will not need to wait until they receive their mailed notification.

We will provide more detailed communications once the hotline is available.

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.