Anthem Security Breach FAQ

How many of my members are impacted?

Anthem is currently conducting an extensive IT forensic investigation to determine what members are impacted. We will provide additional details to our Administrative Services Only (ASO) clients as soon as it is available.

Will you keep me updated on any changes in this situation?

Yes, as we learn more we will keep you updated. We will also update www.anthemfacts.com.

What are you doing to protect the information of Anthem members?

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 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 learned that the compromised database warehouse experienced a series of sporadic suspicious queries during the course of several weeks. Anthem took immediate action to secure its data and contacted federal investigators as soon as it made that discovery.

How many people are impacted?

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. We are still working to identify how many Social Security numbers were accessed.

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, telephone numbers, email addresses and employment information including income data.

Is financial information – credit card, debit card information – part of the information that was compromised?

The data included member income information. However, our investigation to date shows there was no credit card or debit card information compromised.

Was there any diagnosis or treatment data accessed?

No—we do not believe that there was any diagnosis or treatment data exposed.

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 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 did hackers get into the Anthem network/environments?

Our investigation shows the attacker had a proficient understanding of the data platforms and successfully utilized valid illegally-obtained database administrator logon information.

Since they had valid logon information, do you believe the hackers had help from an inside source?

Through our investigation, Anthem was able to rule out any internal resources as the source of the data breach. We continue working with federal investigators to determine who is responsible and why Anthem, Inc. was targeted.

Does this incident affect members as well as anyone who has applied for insurance during open enrollment on the health insurance marketplace?

At this time, we are conducting a thorough IT forensic investigation to determine whose information was accessed. This incident affects members and groups whose data was contained in the database warehouse during the time of the data queries – December 10, 2014 – January 27, 2015.

What measures have you taken to protect against further cyber attacks?

Anthem Information Security has worked to eliminate any further vulnerability and continues 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.

Was this a breach by an internal resource or an external cyber attack?

Through our investigations, Anthem was able to rule out any internal resources as the source of the data breach. We continue working with federal investigators to determine who is responsible and why Anthem, Inc. was targeted.

Who is responsible for this cyber attack?

Anthem is working closely with federal law enforcement investigators. At this time, no one person or entity has been identified as the attacker.

Have you notified law enforcement?

Yes, we notified the FBI and are working closely with federal law enforcement investigators to determine the source of the cyber attack.

Who is involved in the investigation?

Anthem is working directly with federal law enforcement investigators who specialize in cyber attacks.

Are consumer portals impacted?

No, it does not appear that any other databases or networks were compromised. Anthem is continuing to investigate.

Are you going to offer credit monitoring/identity protection services for impacted members?

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 enrolled in identity repair services. In addition, impacted members will be provided information on how to enroll in free credit monitoring.

Is there a website I can go to for more information?

Yes, www.AnthemFacts.com. We will continue to update this site as new information is made available.

Is there a phone number to call for more information?

Yes, it is 1-877-263-7995.

Are you notifying those impacted?

Yes, Anthem is working to identify all who are impacted. Notice to those impacted will be mailed in the coming weeks.

Is this a HIPAA Incident?

Yes, the information disclosed falls under HIPAA.

Was broker data accessed?

Our investigation to date indicates that no broker data was accessed.