

# the *Availability Digest*

[www.availabilitydigest.com](http://www.availabilitydigest.com)  
[@availabilitydig](https://twitter.com/availabilitydig)

## **Anthem Loses 80 Million Records to Hackers**

March 2015

Anthem, Inc. is the second largest health insurer in the United States. Part of the Blue Cross Blue Shield (BCBS) health insurance network, Anthem has almost 40 million customers in fourteen states: California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia, and Wisconsin. Anthem is one of 37 companies that insure 105 million people under the Blue Cross Blue Shield license.



Anthem maintains a database of all of its customers plus any customers of other BCBS plans that received care in an Anthem area.

On Wednesday, February 4<sup>th</sup>, Anthem announced that hackers had breached its IT systems and stole the personal information of up to 78.8 million BCBS customers and employees. This was the largest data breach to date of any U.S. health insurer.

None of this information was encrypted. If Anthem had encrypted its customer data in the database, the hack would have been useless to the attackers.

### **The Anthem Hack**



The Anthem attack was unique in one sense. Most malware that steals data is not discovered by the victim company. Rather, it is reported to the victim by another company. For instance, the theft of payment-card data (such as that experienced by Target during the 2013 holiday season<sup>1</sup>) is often first noticed by one or more issuing banks that experience a sudden increase in fraudulent purchases. In the case of the Anthem hack, however, the discovery was made by an employee.

On January 27<sup>th</sup>, a few days before Anthem announced the attack, an Anthem database administrator discovered a database query running under his login information that he had not initiated. He stopped the query and alerted Anthem's Information Security department. Anthem immediately notified the FBI (the U.S. Federal Bureau of Investigation).

Anthem personnel also discovered that the login information for five other database administrators had been compromised. It was further determined that the attack had been in progress for over a month and a half, since December 10, 2014. It is likely that the database administrators' credentials were obtained via phishing emails that trick users into unwittingly revealing passwords or downloading malicious software.

Fortunately, it appears that no medical information was stolen such as claims, test results, or diagnostic codes, nor was any financial data such as credit-card or bank-account numbers taken. However, the

<sup>1</sup> [Target Compromises Millions of Payment Cards](http://www.availabilitydigest.com/public_articles/0901/target.pdf), *Availability Digest*, January 2014.  
[http://www.availabilitydigest.com/public\\_articles/0901/target.pdf](http://www.availabilitydigest.com/public_articles/0901/target.pdf)

stolen data included names, birthdays, social security numbers, street addresses, email addresses, income data, and BCBS policy numbers. This is sufficient data to open accounts, file fraudulent tax returns, and even to receive medical attention.

## Many Children Were Victims

Tens of millions of the victims were children that were listed on their parents' insurance policies. These children are all subject to identify theft, and there is no straight-forward way for a parent to know of the theft. Because there is typically no history and no credit applications for children, it is easy to fraudulently use their information to open accounts, commit tax fraud, and get medical treatment in the name of a child, leaving the parents saddled with bills and a health record for their child that is no longer accurate.

It can take years for the theft of child information to come to light. It may not be apparent until a child applies for credit and is turned down because of defaulted payments. However, there are red flags that may be raised:

- Collection agency calls or letters for a child.
- Pre-approved credit-card offers for children who have never had a bank account.
- Notice of a traffic violation.
- Notice of overdue taxes.
- Denial of government benefits because the child's social security number is listed as having already received the benefits
- Notification from the IRS that a child's name or social security number appears on someone else's tax return.

## Anthem's Response

Anthem immediately sent an email to all of its members:

"To Our Members:

Safeguarding your personal, financial, and medical information is one of our top priorities, and because of that, we have state-of-the-art information security systems to protect your data.

However, despite our efforts, Anthem Blue Cross Blue Shield was the target of a very sophisticated external cyberattack. These attackers gained unauthorized access to Anthem's IT system and have obtained personal information from our current and former members such as their names, birthdays, medical IDs/social security numbers, street addresses, e-mail addresses and employment information, including income data."

Anthem is working with AllClear ID, a leading identity-protection provider, to provide automatic free credit-monitoring and identify-protection services for 24 months for all current and former members of an affected Anthem plan dating back ten years to 2004. Affected members can also enroll at no cost to AllClear PRO service during the 24-month coverage period. This service provides a \$1 million credit-monitoring and identity-theft insurance policy (the provision of some personal information is required for this service).

Anthem has set up an informational web site at [www.anthemfacts.com](http://www.anthemfacts.com) that discusses how to go about credit freezes and fraud alerts via the three credit bureaus so that no new lines of credit can be opened without a user's permission. It has also established a toll-free number, 877-263-7995, for a dedicated investigator who will work to recover an affected member's financial losses and to restore credit, ensuring that the member's identity is returned to its proper condition.

## Scamming Attacks

The theft of email addresses and other personal information always leads to a rash of scamming attacks. Scammers are sending spam email and calling members claiming to represent Anthem. They are offering a free year of credit-card protection services and in doing so are asking for personal data like social security and credit-card numbers. Anthem has warned:

“These emails are not from Anthem, and no notifications have been sent from Anthem since the initial notification on Wednesday, February 4, 2015.”

Anthem said that it will send a letter and email to everyone whose information was stored in the hacked database. Anthem further said that it will not call any members regarding the cyberattack. Anthem cautioned members as follows:

- Do not reply to any email purportedly from Anthem.
- Do not supply any information on a website that may open if a link is clicked.
- Do not open any attachments that arrive with a purported Anthem email.
- Do not respond to any information from a phone call purportedly from Anthem.

## Lawsuits

The first lawsuits in the Anthem hack have been filed in Indiana, California, Alabama, and Georgia. The suits allege that Anthem did not take adequate and reasonable measures to ensure its data systems were protected

## Pointing the Finger

Following the attack on the U.S. hospital group Community Health Systems, in which tens of millions of patients' health records were stolen, the FBI has warned that the \$3 trillion U.S. healthcare industry is being increasingly targeted. Many health-care companies are still reliant on ageing legacy systems that do not use the latest security measures.

Medical identity theft is often more valuable than credit-card theft. Credit cards can be quickly canceled by banks when fraudulent transactions show up, but medical identity theft is often not immediately identified by patients or their providers. Criminals have years to milk such credentials.

The FBI has confirmed that it is close to discovering who is behind the Anthem attack, but they will not confirm any suspect until the agency is absolutely sure. In the past, they have pointed their finger at China, accusing it of attacking U.S. companies and consumers.

## Summary

It was fortunate that Anthem discovered the attack fairly immediately (it seems that a month and a half is sadly a fairly short time for discovery of hacking attacks). However, this was enough time for the hackers to compromise their entire database of members and employees.

What is unfortunate is that none of Anthem's sensitive database was encrypted in place. Hacking attacks are going to stop only when corporations make the investment to incorporate encryption into their systems so that stolen information has no value. True, this can be a costly move. However, its cost must be compared to the cost and publicity that accompanies a major hack such as the Anthem attack.

## Acknowledgements

Information for this article was obtained from the following sources:

[Anthem Hacked, Millions of Records Likely Stolen](#), *Huffington Post*, February 4, 2015.  
[Who's to blame for the Anthem hack?](#) *CNN*, February 6, 2015.

First lawsuits launched in Anthem hack, *USA Today*; February 8, 2015.  
Anthem Hack: What You Need to Do to Protect Yourself, *ABC News*; February 8, 2015.  
Anthem hack leaves room for scammers to pounce, *Christian Science Monitor*; February 11, 2015.  
There are two key lessons that IT can learn from the Anthem breach, *Information Week*; February 12, 2015.  
China To Blame in Anthem Hack?, *Krebs on Security*; February 15, 2015.  
Kids Get Hurt by Anthem Security Breach, *Daily Finance*; February 19, 2015.  
FBI “close” to identifying Anthem hackers, as dozens of state-sponsored groups identified, *ZD Net*; February 24, 2015.  
Anthem Hack: Millions of Non-Anthem Customers Could Be Victims, *NBC News*; February 24, 2015.  
Anthem says at least 8.8 million non-customers could be victims in data hack, *Yahoo*; February 28, 2015.  
How to Access & Sign Up for Identity Theft Repair & Credit Monitoring Services, *Anthem*; February 13, 2015. [www.anthemfacts.com](http://www.anthemfacts.com)