

# The Anthem Customer and Employee Data Breach

Prepared by Dick Smith, Training Director of Computer Concepts from technical sources, news articles and the Anthem's web site.

On February 4, 2015, Anthem, the second largest U.S. health insurer, announced that one of its IT systems had been breached, resulting in the loss of customer and employee information including income data.

The Anthem cyber-attack is the biggest known infiltration of an American healthcare provider affecting approximately 80 million insured members.

Joseph Swedish, the Anthem President and CEO has stated that Anthem is working to identify the members who have been affected by the security breach. Mr. Swedish described the hack as a "very sophisticated external cyber-attack."

Mandiant, one of the world's leading cybersecurity firms, has been retained by Anthem and according to Anthem, Mandiant is working around the clock to do everything they can to further secure Anthem's customers' data.

Anthem has created a dedicated website at AnthemFacts.com and for current and former members, a toll-free number: 1-877-263-7995.

Anthem plans affected are Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, Caremore, Unicare, Healthlink, and DeCare.

The information stolen includes personal information from current and former members. Medical records were not taken, but information such as names, birthdays, medical IDs/Social Security numbers, street addresses, email addresses and employment information, including income data, according to the company's email.

## **Defensive Tips**

- Visit the AnthemFacts.com web site.
- Change passwords for all email accounts, financial accounts and social media accounts.
- Go to FreeCreditReport.com to obtain your yearly free credit report from credit reporting agencies Equifax, TransUnion and Experian. Be sure to place a fraud alert on the report.
- Monitor financial transactions such as credit and debit card accounts for fraudulent transactions and report any suspicious transactions to your credit card companies
- File your taxes as soon as possible. The IRS and local governments are not prepared to know the difference in a tax form from you or someone impersonating you.

## **Anthem Won't Be the Last**

"A sad fact is that the healthcare industry by and large has never been seen as a leading edge security consumer because the historical threat has been more focused on financial services," said Mark Krainak, Chief Product Officer for Imperva. "This is a broad generalization but healthcare targets are probably a little bit softer targets than financial targets."

There is a good chance other health insurance organizations are already compromised and don't even know it.

---

This article was not created to be a comprehensive document regarding the Anthem event.