To Members:

On January 29, 2015, Anthem, Inc. (Anthem) discovered that cyber attackers executed a sophisticated attack to gain unauthorized access to Anthem's IT system and obtained personal information relating to consumers who were or are currently covered by Anthem or other independent Blue Cross and Blue Shield plans that work with Anthem. Anthem believes that this suspicious activity may have occurred over the course of several weeks beginning in early December, 2014.

As soon as we discovered the attack, we immediately began working to close the security vulnerability and contacted the FBI. We have been fully cooperating with the FBI's investigation. Anthem has also retained [redacted] one of the world's leading cybersecurity firms, to assist us in our investigation and to strengthen the security of our systems.

Consumers Impacted
Current or former members of one of Anthem's affiliated health plans may be impacted. In addition, some members of other independent Blue Cross and Blue Shield plans who received healthcare services through the BlueCard program in any of the areas that Anthem serves over the last 10 years may be impacted. The Blue Cross and Blue Shield Association's BlueCard program is a national program that enables members of one Blue Cross and Blue Shield Plan to obtain healthcare services while traveling or living in another Blue Cross and Blue Shield Plan's service area. Anthem is providing identity protection services to all individuals that are impacted. For a listing of potentially impacted Anthem affiliated health plans and other Blue Cross and Blue Shield companies for which Anthem provides services under the BlueCard program, visit Anthem-Facts.com to view a list. You are receiving this message from Anthem as a current or former member of one of these potentially impacted companies.

Information Accessed
The information accessed may have included names, dates of birth, Social Security numbers, health care ID numbers, home addresses, email addresses, employment information, including income data. We have no reason to believe credit card or banking information was compromised, nor is there evidence at this time that medical information such as claims, test results, or diagnostic codes, was targeted or obtained.

BLAH BLAH BLAH !

The bottom line is they’re saying...

We’re Sorry...

We sorry that doing business with us has screwed you. We’re sorry your privacy is gone. We’re sorry your information is being sold all over the world and there are now 350 people with your name and social creating fake identities and you can’t do squat about it.

We’re sooooo Sorry... please don’t make the government hurt us.