

## Anthem Breach

### FAQ for Students:

- Anthem was the target of a very sophisticated external cyber attack.
- It is not yet determined that Pepperdine student enrollments have been breached.
- These cyber attackers gained unauthorized access to Anthem's Information Technology (IT) system and have obtained personal information from its current and former members such as their names, birthdays, member health ID numbers/Social Security numbers, street addresses, email addresses and employment information, including income data.

Note: In the event that student information has been breached the following is important to know: Student accounts with Anthem do not transmit Social Security Numbers or credit card information, so neither of those data sets will be compromised. Anthem reports that no financial data has been compromised and Anthem also does not believe any medical data has been obtained. Anthem's investigation to date indicates there is no evidence that credit card or medical information, such as claims, test results, or diagnostic codes were targeted or compromised.

- Once the attack was discovered, Anthem immediately made every effort to close the security vulnerability, contacted the Federal Bureau of Investigation (FBI) and began fully cooperating with their investigation. Anthem has also retained Mandiant, one of the world's leading cybersecurity firms, to provide incident response and security assessment services.
- Anthem is not aware of any fraud that has occurred as a result of this incident against its 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.
- Anthem has created a dedicated website ([www.AnthemFacts.com](http://www.AnthemFacts.com)) where you and other members can access information such as frequently asked questions and answers and a telephone number that members can call 1-877-263-7995.

## Member FAQ

### **Was my information accessed?**

Anthem is currently conducting an extensive IT forensic investigation to determine what members are impacted. The Anthem teams are working around the clock to determine how many people have been impacted and will notify all Anthem members who are impacted through a written communication.

### **What information was compromised?**

Anthem's Initial investigation indicates that the member data accessed included names, dates of birth, member health ID numbers/Social Security numbers, addresses, telephone numbers, email addresses and employment information including income data.

### **Was there any diagnosis or treatment data exposed?**

Anthem's investigation to date indicates there is no evidence that medical information, such as claims, test results, or diagnostic codes were targeted or compromised.

**Was my credit card information accessed?**

Anthem's investigation to date indicates there is no evidence that credit card information was compromised.

**Do the people who accessed my information have my Social Security number?**

Anthem's investigation to date indicates that the information accessed included names, dates of birth, member health ID numbers/Social Security numbers, street addresses, email addresses and employment information. Anthem is working to determine whose Social Security numbers were accessed.

**How can I sign up for credit monitoring services?**

All impacted members will receive notice via mail which will advise them of the protections being offered to them as well as any next steps.

**When will I receive my letter in the mail?**

We continue working to identify the members who are impacted. We expect the mailing of letters to begin in the next two weeks.

**My children are on my insurance plan, was their information also accessed?**

Anthem is currently conducting an extensive IT forensic investigation to determine which members are impacted; however, adults and children were impacted.

**Do the people who accessed my information know about my medical history?**

Our investigation to date indicates there was no diagnosis or treatment data exposed.

**Do the people who accessed my information have my credit card numbers and banking information?**

No, the investigation to date indicates that information accessed did not include credit card numbers, banking or other financial information.

**Has anyone used my information yet?**

We are not aware of any fraud that has occurred as a result of this incident against our members.

**Am I at risk for identity theft?**

Anthem is currently conducting an extensive IT forensic investigation to determine which members are impacted. 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.

**Do I need a new member ID card and number?**

Anthem is working around the clock to determine how many people have been impacted and will notify all who are impacted. Anthem will provide further guidance on next steps.

**How can I be sure my personal and health information is safe with Anthem, Inc.?**

Safeguarding its members' personal, financial and medical information is a top priority for Anthem, and because of that, they 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 is Anthem doing to help members potentially affected by this incident?**

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.

**Where is the data now? And who can access my information?**

Evidence indicates that the data was uploaded to an external file sharing service. This file sharing service, at Anthem's request, has locked down the account and data so that it cannot be copied, accessed or removed. Anthem and the FBI are working with the file sharing service to access the data and further secure it.