

1 **FITAPELLI & SCHAFFER, LLP**

2 Joseph A. Fitapelli
3 Brian S. Schaffer
4 Nicholas P. Melito
4 475 Park Avenue South, 12th Floor
5 New York, New York 10016
6 Telephone: (212) 300-0375

15 CV 920

JUDGE OCTAVIO

7 [Additional Attorneys on Signature Page]

8 **UNITED STATES DISTRICT COURT**
9 **SOUTHERN DISTRICT OF NEW YORK**

10 ALEX SCHNEIDER and FRANK
11 PACILIO, JR. individually and on behalf of
12 all others similarly situated,

13 Plaintiffs,

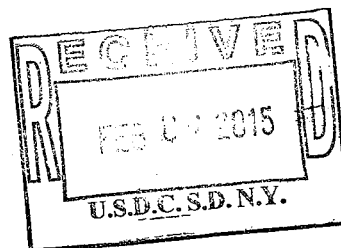
14 vs.

15 ANTHEM, INC., d/b/a Anthem Health,
16 Inc., an Indiana Corporation, THE
17 ANTHEM COMPANIES, INC., an Indiana
18 Corporation, THE ANTHEM
19 COMPANIES OF CALIFORNIA, INC., a
20 California Corporation, and ANTHEM
21 BLUE CROSS LIFE AND HEALTH
22 INSURANCE COMPANY, a California
23 Corporation,

24 Defendants.

CASE NO. _____

CLASS ACTION COMPLAINT FOR:



DEMAND FOR JURY TRIAL

1 Plaintiffs Alex Schneider and Frank Pacilio, Jr. (collectively, "Plaintiffs") bring
2 this class action against Defendants ANTHEM, INC., d.b.a Anthem Health, Inc., an
3 Indiana Corporation, THE ANTHEM COMPANIES, INC., an Indiana Corporation,
4 THE ANTHEM COMPANIES OF CALIFORNIA, INC., a California Corporation,
5 and ANTHEM BLUE CROSS LIFE AND HEALTH INSURANCE COMPANY, a
6 California Corporation (collectively, "ANTHEM" or DEFENDANTS), as a result of
7 the massive data breach suffered by as many as 80 million ANTHEM customers, on
8 behalf of themselves and all others similarly situated to obtain damages, restitution and
9 injunctive relief for the Class, as defined below, from Defendants. Plaintiffs make the
10 following allegations upon information and belief, except as to their own actions, the
11 investigation of their counsel, and the facts that are a matter of public record:
12
13
14
15

16 NATURE OF CLAIM

17 1. This is a consumer class action lawsuit brought on behalf of Plaintiffs,
18 individually, and on behalf of all other individuals, against Defendants for their failure
19 to safeguard and secure the medical records, and other personally identifiable
20 information, including names, dates of birth, social security numbers, billing
21 information, and highly confidential health and other types of information (collectively
22 "Personally Identifiable Information" or "PII") and personal health related information
23 (collectively "Personal Health Information" or "PHI") of Plaintiffs and Class
24 Members. PHI and PII shall also be referred to collectively as Personal Information.
25 Defendants announced to the public this massive loss of information on or about
26
27
28

1 February 4, 2015.

2 2. Defendants failed to keep safe their customers' sensitive private,
3 financial, medical and personal information.
4

5 **PARTIES**

6 3. Plaintiff Alex Schneider ("Schneider") is an individual who resides in this
7 District and is a customer of Defendants.
8

9 4. Plaintiff Frank Pacilio, Jr. ("Pacilio") is an individual who resides in the
10 Eastern District and is a customer of Defendants.
11

12 5. Defendant ANTHEM, INC., d/b/a ANTHEM HEALTH, INC. is an
13 Indiana Corporation, registered with the California Secretary of State to do business in
14 California, and headquartered in Indianapolis, Indiana.
15

16 6. Defendant THE ANTHEM COMPANIES, INC. is an Indiana
17 Corporation, registered with the California Secretary of State to do business in
18 California, and headquartered in Indianapolis, Indiana.
19

20 7. Defendant THE ANTHEM COMPANIES OF CALIFORNIA, INC. is a
21 California Corporation and headquartered in Indianapolis, Indiana.
22

23 8. Defendant ANTHEM BLUE CROSS LIFE AND HEALTH
24 INSURANCE COMPANY is a California Corporation and headquartered in
25 Indianapolis, Indiana.
26
27
28

1 **JURISDICTION AND VENUE**

2 9. This Court has original jurisdiction pursuant to 28 U.S.C. §1332(d)(2). In
3 the aggregate, Plaintiffs' claims and the claims of the other members of the Class
4 exceed \$5,000,000 exclusive of interest and costs, and there are numerous class
5 members who are citizens of states other than Defendants' states of citizenship, which
6 are Indiana and California.
7

8
9 10. This Court has personal jurisdiction over ANTHEM because ANTHEM is
10 authorized to do and does business in the State of New York.
11

12 11. Venue is proper in this Court pursuant to 28 U.S.C. §1391 because many
13 of the acts and transactions giving rise to this action occurred in this District and
14 because ANTHEM is subject to personal jurisdiction in this District.
15

16 **GENERAL ALLEGATIONS**

17 12. ANTHEM, INC., previously known as WellPoint, Inc., is one of the
18 largest for-profit managed health care companies in the United States.
19

20 13. Plaintiffs have health insurance issued by ANTHEM, and as a result,
21 Anthem has required that Plaintiffs provide their PHI and PII to Anthem.
22

23 14. ANTHEM claims that on or about January 29, 2015, it detected a massive
24 data breach that compromised the PHI and PII of approximately 80 million insureds.
25

26 15. News of the data breach was first published by the Wall Street Journal at
27 <http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720> (last
28 visited Feb. 5, 2014).

1 16. ANTHEM does not provide any information as to when its systems were
2 compromised, how long third parties had access to its systems or what measures have
3 been taken to prevent further breaches.
4

5 17. ANTHEM does not definitely state that customers' banking and medical
6 information was not disclosed to third parties.
7

8 18. Medical information of ANTHEM'S customers, such as claims, test
9 results, medical history, and diagnoses were also compromised and disclosed to third
10 parties.
11

12 19. The banking and credit information of ANTHEM'S customers were also
13 compromised and disclosed to third parties.
14

15 20. ANTHEM also set up a website at <www.anthemfacts.com> where the
16 data breach was disclosed to ANTHEM customers by way of a letter from Joseph R.
17 Swedish, President and CEO of ANTHEM. This website also provides a short and
18 vague facts page at <www.anthemfacts.com/faq> (last visited February 6, 2015);
19 attached as Exhibit A.
20

21 21. On that website, ANTHEM states that "all product lines [were]
22 impacted." *See* Exhibit A.
23

24 22. On information and belief, Plaintiffs' PHI and PII was disclosed in the
25 data breach.
26
27
28

CONSEQUENCES OF DEFENDANTS' CONDUCT

1
2 23. The ramifications of Defendants' failure to keep class members' PHI and
3 PII are severe.

4
5 24. The information Defendants lost, including Plaintiffs' PHI and PII, is "as
6 good as gold" to identity thieves, in the words of the Federal Trade Commission
7 ("FTC"). FTC, *About Identity Theft*, available at
8 <<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>>
9 (visited February 5, 2015). Identity theft occurs when someone uses another's
10 personal identifying information, such as that person's name, address, credit card
11 number, credit card expiration dates, and other information, without permission, to
12 commit fraud or other crimes. *Id.* The FTC estimates that as many as 9 million
13 Americans have their identities stolen each year. *Id.*

14
15 25. Identity thieves can use identifying data to open new financial accounts
16 and incur charges in another person's name, take out loans in another person's name,
17 incur charges on existing accounts, or clone ATM, debit, or credit cards. *Id.*

18
19 26. Identity thieves can use PHI and PII such as that pertaining to the Class,
20 which Defendants failed to keep secure to perpetrate a variety of crimes that do not
21 cause financial loss, but nonetheless harm the victims. For instance, identity thieves
22 may commit various types of government fraud such as: immigration fraud; obtaining
23 a driver's license or identification card in the victim's name but with another's picture;
24 using the victim's information to obtain government benefits; or filing a fraudulent tax
25
26
27
28

1 return using the victim's information to obtain a fraudulent refund.

2 27. In addition, identity thieves may get medical services using the Plaintiffs'
3 PHI and PII or commit any number of other frauds, such as obtaining a job, procuring
4 housing, or even giving false information to police during an arrest.
5

6 28. Annual monetary losses from identity theft are in the billions of dollars.

7
8 According to a Presidential Report on identity theft produced in 2008:

9 In addition to the losses that result when identity thieves
10 fraudulently open accounts or misuse existing accounts, . . . individual
11 victims often suffer indirect financial costs, including the costs incurred in
12 both civil litigation initiated by creditors and in overcoming the many
13 obstacles they face in obtaining or retaining credit. Victims of non-
14 financial identity theft, for example, health-related or criminal record
15 fraud, face other types of harm and frustration.

16 In addition to out-of-pocket expenses that can reach thousands of
17 dollars for the victims of new account identity theft, and the emotional toll
18 identity theft can take, some victims have to spend what can be a
19 considerable amount of time to repair the damage caused by the identity
20 thieves. Victims of new account identity theft, for example, must correct
21 fraudulent information in their credit reports and monitor their reports for
22 future inaccuracies, close existing bank accounts and open new ones, and
23 dispute charges with individual creditors.

24 *The President's Identity Theft Task Force Report* at p.21 (Oct. 21, 2008),
25 available at <<http://www.idtheft.gov/reports/StrategicPlan.pdf>>.

26 29. According to the U.S. Government Accountability Office ("GAO"),
27 which conducted a study regarding data breaches:

28 [L]aw enforcement officials told us that in some cases, stolen data may be
held for up to a year or more before being used to commit identity theft.
Further, once stolen data have been sold or posted on the Web, fraudulent
use of that information may continue for years. As a result, studies that
attempt to measure the harm resulting from data breaches cannot
necessarily rule out all future harm.

1
2 GAO, *Report to Congressional Requesters*, at p.33 (June 2007), available at
3 <<http://www.gao.gov/new.items/d07737.pdf>>.

4 30. “In addition to the financial harm associated with other types of identity
5 theft, victims of medical identity theft may have their health endangered by inaccurate
6 entries in their medical records. This inaccurate information can potentially cause
7 victims to receive improper medical care, have their insurance depleted, become
8 ineligible for health or life insurance, or become disqualified from some jobs. Victims
9 may not even be aware that a theft has occurred because medical identity theft can be
10 difficult to discover, as few consumers regularly review their medical records, and
11 victims may not realize that they have been victimized until they receive collection
12 notices, or they attempt to seek medical care themselves, only to discover that they
13 have reached their coverage limits.” *Id.* at 30.

14
15
16
17
18 31. “With the advent of the prescription drug benefit of Medicare Part D, the
19 Department of Health and Human Services’ Office of the Inspector General (HHS
20 OIG) has noted a growing incidence of health care frauds involving identity theft.”
21 Identity thieves can use such information “fraudulently to enroll unwilling
22 beneficiaries in alternate Part D plans in order to increase . . . sales commissions” or
23 commit other types of fraud. “The types of fraud that can be perpetrated by an identity
24 thief are limited only by the ingenuity and resources of the criminal.” *Id.* at 31.

25
26
27 32. According to the U.S. Government Accountability Office (“GAO”),
28

1 which conducted a study regarding data breaches:

2 [L]aw enforcement officials told us that in some cases, stolen data may be held
3 for up to a year or more before being used to commit identity theft. Further,
4 once stolen data have been sold or posted on the Web, fraudulent use of that
5 information may continue for years. As a result, studies that attempt to measure
6 the harm resulting from data breaches cannot necessarily rule out all future
7 harm.

8 GAO, *Report to Congressional Requesters*, at p.33 (June 2007), available at
9 <<http://www.gao.gov/new.items/d07737.pdf>>.

10 33. The unauthorized disclosure of Social Security Numbers can be
11 particularly damaging, because Social Security Numbers cannot easily be replaced. In
12 order to obtain a new number, a person must prove, among other things, that he or she
13 continues to be disadvantaged by the misuse. Thus, no new number can be obtained
14 until the damage has been done. Furthermore, as the Social Security Administration
15 (“SSA”) warns:

16 a new number probably will not solve all your problems. This is because other
17 governmental agencies (such as the Internal Revenue Service and state motor
18 vehicle agencies) and private businesses (such as banks and credit reporting
19 companies) likely will have records under your old number. Also, because
20 credit reporting companies use the number, along with other personal
21 information, to identify your credit record, using a new number will not
22 guarantee you a fresh start. This is especially true if your other personal
23 information, such as your name and address, remains the same.

24 If you receive a new Social Security Number, you will not be able to use the old
25 number anymore.

26 For some victims of identity theft, a new number actually creates new problems.
27 If the old credit information is not associated with the new number, the absence
28 of any credit history under the new number may make it more difficult for you

1 to get credit.

2
3 SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064
4 (Aug. 2009), available at <<http://www.ssa.gov/pubs/10064.html>>.

5
6 34. Plaintiffs and the Class they seek to represent now face years of constant
7 surveillance of their financial and medical records, monitoring, loss of rights, and
8 potential medical problems.
9

10 **CLASS ACTION ALLEGATIONS**

11 35. Plaintiffs bring this action on their own behalf, and on behalf of all other
12 persons similarly situated (“the Class”). The Class that Plaintiffs seek to represent is:
13

14 All persons who have purchased health insurance from Anthem, Inc.
15 d/b/a Anthem Health, Inc., The Anthem Companies, Inc., The Anthem
16 Companies of California, and Anthem Blue Cross Life and Health
17 Insurance Company and whose personal and/or financial information
18 was breached as a result of the data breach announced on or about
19 February 4, 2015.

20 Excluded from the Class are Defendants; officers, directors, and
21 employees of Defendants; any entity in which Defendants have a
22 controlling interest; the affiliates, legal representatives, attorneys,
23 heirs, and assigns of the Defendants.

24 36. The members of the Class are so numerous that the joinder of all members
25 is impractical. While the exact number of Class members is unknown to Plaintiffs at
26 this time, based on information and belief, it is in the millions.

27 37. There is a well-defined community of interest among the members of the
28 Class because common questions of law and fact predominate, Plaintiffs’ claims are

1 typical of the members of the Class, and Plaintiffs can fairly and adequately represent
2 the interests of the Class.

3
4 38. This action satisfies the requirements of Federal Rule of Civil Procedure
5 23(b)(3) because it involves questions of law and fact common to the member of the
6 Class that predominate over any questions affecting only individual members,
7 including, but not limited to:

- 8
- 9 a. Whether Defendants unlawfully used, maintained, lost or disclosed
10 Class members' PHI and PII;
 - 11 b. Whether ANTHEM unreasonably delayed in notifying affected
12 customers of the data breach;
 - 13 c. Whether Defendants failed to implement and maintain reasonable
14 security procedures and practices appropriate to the nature and
15 scope of the information compromised in the data breach.
 - 16 d. Whether, by the misconduct set forth herein, Defendants violated
17 consumer protection statutes and/or state deceptive business
18 practices statutes;
 - 19 e. Whether Defendants' conduct was negligent;
 - 20 f. Whether Defendants acted willfully and/or with oppression, fraud,
21 or malice;
 - 22 g. Whether Defendants' conduct constituted Intrusion;
 - 23 h. Whether Defendants' conduct constituted Public Disclosure of
24
25
26
27
28

1 Private Facts;

2 i. Whether Defendants' conduct constituted Misappropriation of
3 Likeness and Identity;

4 j. Whether Defendants' conduct constituted Bailment;

5 k. Whether Defendants' conduct constituted Conversion;

6 l. Whether Defendants unlawfully used, maintained, lost or disclosed
7 Class members' PHI and PII; and

8 m. Whether Plaintiffs and the Class are entitled to damages, civil
9 penalties, punitive damages, and/or injunctive relief.

10 39. Plaintiffs' claims are typical of those of other members of the Class
11 because Plaintiffs' PHI and PII, like that of every other class member, was misused
12 and/or disclosed by Defendants.

13 40. Plaintiffs will fairly and accurately represent the interests of the Class.
14 Plaintiffs have retained competent and capable attorneys with significant experience in
15 complex and class action litigation, including consumer class actions. Plaintiffs and
16 their counsel are committed to prosecuting this action vigorously on behalf of the Class
17 and have the financial resources to do so. Neither Plaintiffs nor their counsel have
18 interests that are contrary to or that conflict with those of the proposed Class.

19 41. The prosecution of separate actions by individual members of the Class
20 would create a risk of inconsistent or varying adjudications with respect to individual
21 members of the Class, which would establish incompatible standards of conduct for
22
23
24
25
26
27
28

1 Defendants and would lead to repetitive adjudication of common questions of law and
2 fact. Accordingly, class treatment is superior to any other method for adjudicating the
3 controversy. Plaintiffs know of no difficulty that will be encountered in the
4 management of this litigation that would preclude its maintenance as a class action
5 under Rule 23(b)(3).
6

7
8 42. Damages for any individual class member are likely insufficient to justify
9 the cost of individual litigation, so that in the absence of class treatment, Defendants'
10 violations of law inflicting substantial damages in the aggregate would go un-remedied
11 without certification of the Class.
12

13 43. Defendants have acted or refused to act on grounds that apply generally to
14 the class, as alleged above, and certification is proper under Rule 23(b)(2).
15

16 FIRST COUNT

17 **Breach of GBL § 349 and the Various Analogous State Consumer Laws**

18 **(Against all Defendants)**

19
20 44. Plaintiffs incorporate the substantive allegations contained in all previous
21 paragraphs as if fully set forth herein.
22

23 45. Defendants' transactions with Plaintiffs and the Class as described herein
24 constitute the "conduct of any trade or commerce" within the meaning of NYS GBL §
25 349.
26

27 46. Further, Defendants' transactions with Plaintiffs and the Class as
28 described herein constitute "unfair or deceptive acts or practices in the conduct of any

1 trade or commerce” between a business and consumers within the meaning of NYS
2 GBL § 349.

3
4 47. Defendants in the normal course of their business collected customer
5 information.

6 48. Defendants misrepresented the safety and security of their data collection
7 and retention systems.

8
9 49. Defendants failed to use proper data encryption to secure their members’
10 Personal Information.

11
12 50. The foregoing acts and conduct of Defendants are deceptive in that they
13 represented to the Class that such Personal Information would remain secure and/or
14 that they had the technology or policies to secure financial transaction information
15 when Defendants did not have adequate security measures.

16
17 51. Defendants’ failure to disclose information concerning the data breach
18 directly and promptly to affected customers, constitutes a fraudulent act or practice in
19 violation NYS GBL § 349.

20
21 52. Plaintiffs suffered injury in fact and lost property and money as a result of
22 Defendants’ conduct.

23
24 53. Plaintiff seeks restitution and injunctive relief on behalf of the Class.
25
26
27
28

1 **SECOND COUNT**

2 **Negligence**

3 **(Against All Defendants)**

4
5 54. Plaintiffs incorporate the substantive allegations contained in all previous
6 paragraphs as if fully set forth herein.
7

8 55. Defendants came into possession of Plaintiffs' Private Information and
9 had a duty to exercise reasonable care in safeguarding and protecting such information
10 from being compromised, lost, stolen, misused, and/or disclosed to unauthorized
11 parties.
12

13 56. Defendants had a duty to timely disclose that Plaintiffs' Private
14 Information within its possession had been compromised.
15

16 57. Defendants had a duty to have procedures in place to detect and prevent
17 the loss or unauthorized dissemination of Plaintiffs' Private Information.
18

19 58. Defendants, through their actions and/or omissions, unlawfully breached
20 their duty to Plaintiffs by failing to exercise reasonable care in protecting and
21 safeguarding Plaintiffs' Private Information within Defendants' possession.
22

23 59. Defendants, through their actions and/or omissions, unlawfully breached
24 their duty to Plaintiffs by failing to exercise reasonable care by failing to have
25 appropriate procedures in place to detect and prevent dissemination of Plaintiffs'
26 Private Information.
27

28 60. Defendants, through their actions and/or omissions, unlawfully breached

1 their duty to timely disclose to Plaintiffs and the Class members the fact that their
2 Private Information within their possession had been compromised.

3
4 61. Defendants' negligent and wrongful breach of their duties owed to
5 Plaintiffs and the Class proximately caused Plaintiffs' and Class members' Private
6 Information to be compromised.

7
8 62. Plaintiffs seek the award of actual damages on behalf of the Class.

9 **THIRD COUNT**

10 **Bailment**

11 **(Against All Defendants)**

12
13 63. Plaintiffs incorporate the substantive allegations contained in all previous
14 paragraphs as if fully set forth herein.

15
16 64. Plaintiffs and the Class members delivered and entrusted their Private
17 Information to Defendants for the sole purpose of receiving services from Defendants.

18
19 65. During the time of bailment, Defendants owed Plaintiffs and the Class
20 members a duty to safeguard this information properly and maintain reasonable
21 security procedures and practices to protect such information. Defendants breached
22 this duty.

23
24 66. As a result of these breaches of duty, Plaintiffs and the Class members
25 have suffered harm.

26
27 67. Plaintiffs seek actual damages on behalf of the Class.

1 **PRAYER FOR RELIEF**

2 WHEREFORE Plaintiffs pray for judgment as follows:

3
4 A. For an Order certifying this action as a class action and appointing
5 Plaintiffs and their Counsel to represent the Class;

6
7 B. For equitable relief enjoining Defendants from engaging in the wrongful
8 conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs'
9 and Class members' Private Information, and from refusing to issue prompt, complete
10 and accurate disclosures to Plaintiffs and Class members;

11
12 C. For equitable relief requiring restitution and disgorgement of the revenues
13 wrongfully retained as a result of Defendants' wrongful conduct;

14
15 D. For an award of actual damages, compensatory damages, statutory
16 damages, and statutory penalties, in an amount to be determined;

17 E. For an award of punitive damages;

18
19 F. For an award of costs of suit and attorneys' fees, as allowable by law; and

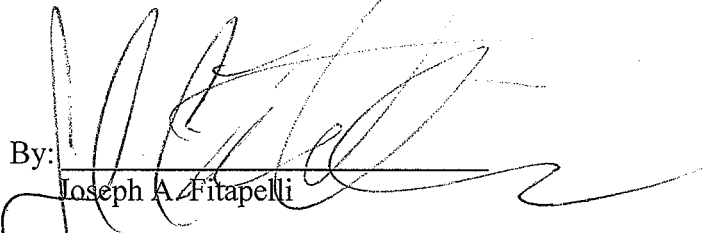
20 G. Such other and further relief as this court may deem just and proper.

21 **DEMAND FOR JURY TRIAL**

22 Plaintiffs hereby demand a jury trial of their claims to the extent authorized by
23 law.
24

25 RESPECTFULLY SUBMITTED AND DATED this 9th day of February, 2015.
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

By: 
Joseph A. Fitapelli

FITAPELLI & SCHAFFER, LLP

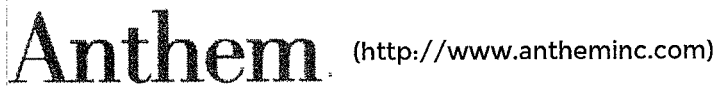
Joseph A. Fitapelli
Brian S. Schaffer
Nicholas P. Melito
475 Park Avenue South, 12th Floor
New York, New York 10016
Telephone: (212) 300-0375

TERRELL MARSHALL DAUDT & WILLIE PLLC

Beth E. Terrell, *pro hac vice motion forthcoming*
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
Telephone: (206) 816-6603

Attorneys for Plaintiffs and the Proposed Class

EXHIBIT "A"



[READ THE FAQ \(./faq\)](#)

**From the Desk
of Joseph R. Swedish**
President and CEO Anthem, Inc.

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 was the target of a very sophisticated external cyber attack. 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, email addresses and employment information, including income data. Based on what we know now, 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 FBI and began fully cooperating with their investigation. Anthem has also retained Mandiant, one of the world's leading cybersecurity firms, to evaluate our systems and identify solutions based on the evolving landscape.

Anthem's own associates' personal information - including my own - was accessed during this security breach. We join you in your concern and frustration, and I assure you that we are working around the clock to do everything we can to further secure your data.

Anthem will individually notify current and former members whose information has been accessed. We will provide credit monitoring and identity protection services free of charge so that those who have been affected can have peace of mind. We have created a dedicated website - www.AnthemFacts.com (<http://www.AnthemFacts.com>) - where members can access information such as frequent questions and answers. We have also established a dedicated toll-free number that both current and former members can call if they have questions related to this incident. That number is: 1-877-263-7995. As we learn more, we will continually update this website and share that information with you.

I want to personally apologize to each of you for what has happened, as I know you expect us to protect your information. We will continue to do everything in our power to make our systems and security processes better and more secure, and hope that we can earn back your trust and confidence in Anthem.

Sincerely,

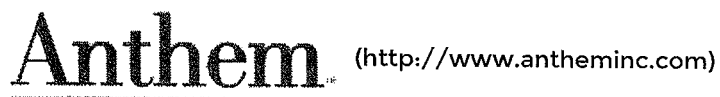
Joseph R. Swedish
President and CEO
Anthem, Inc.

Still have more questions?

READ THE FAQ
(./faq)

©2005-2015 Anthem, Inc. All Rights Reserved. Legal
(<http://www.antheminc.com/Legal/index.htm>) | Privacy
(<http://www.antheminc.com/Privacy/index.htm>)

Updated: 11:45, 02/06/2015



READ THE SPECIAL
MESSAGE FROM JOSEPH
R. SWEDISH (/)

Frequently Asked Questions

**Learn more about the cyber attack
against Anthem**

Was my information accessed?

Anthem is currently conducting an extensive IT Forensic Investigation to determine what members are impacted. We 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 has been compromised?

Initial investigation indicates that the member data accessed included names, dates of birth, member ID/ social security numbers, addresses, phone numbers, email addresses and employment information.

Who is responsible for this cyber attack or breach?

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

When will I receive my letter in the mail?

We continue working to identify the members who are impacted. We will begin to mail letters to impacted members in the coming weeks.

How can I sign up for credit monitoring/identity protection 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.

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

No - 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?

No, our current investigation shows the information accessed did not include credit card numbers.

Did this impact all lines of Anthem Business?

Yes, all product lines are impacted.

Is my (plan/brand) impacted?

The impacted (plan/brand) include 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.

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

Anthem is doing everything it can to ensure there is no further vulnerability to its database warehouses. Anthem has contracted with a global company specializing in the investigation and resolution of cyber attacks. We will work with this company to reduce the risk of any further vulnerabilities and work to strengthen security.

Does this impact Blue Cross and Blue Shield plans not owned by Anthem?

Yes, BlueCard members are impacted. The Blue Cross and Blue Shield Association's BlueCard 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. The program links participating healthcare providers with the independent Blue Cross and Blue Shield Plans across the country and in more than 200 countries and territories worldwide through a single electronic network for claims processing and reimbursement.

I received a call from Anthem related to this cyber attack asking for my information, what should I do?

We are not making any outbound calls to members regarding the cyber attack. 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.

©2005-2015 Anthem, Inc. All Rights Reserved.
Legal (<http://www.antheminc.com/Legal/index.htm>) | Privacy
(<http://www.antheminc.com/Privacy/index.htm>)

Updated: 11:45, 02/06/2015