UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
SOUTHERN DIVISION

EARL EDWARD SCOFIELD, III, individually, and on behalf of all others similarly situated, Plaintiff, vs. ANTHEM, INC., and ANTHEM INSURANCE COMPANIES, INC. d/b/a ANTHEM BLUE CROSS AND BLUE SHIELD, Defendants.	CASE NO. _____ CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Plaintiff Earl Edward Scofield, III ("Plaintiff") brings this class action against Defendants Anthem, Inc., and Anthem Insurance Companies, Inc. d/b/a Anthem Blue Cross and Blue Shield (collectively, "Anthem" or "Defendants"), as a result of the massive data breach suffered by as many as 80 million Anthem customers, many of whom reside in North Carolina, on behalf of himself and all others similarly situated seeking damages, restitution, and injunctive relief for the Class, as defined below, from Defendants.

NATURE OF CLAIM

1. This is a consumer class action lawsuit brought against Defendants for their failure to safeguard and secure the medical records and other personally identifiable information, including names, dates of birth, social security numbers, billing information, and highly confidential health and other types of information ("Personally Identifiable Information" or "PII") and personal health related information ("Personal Health Information" or "PHI") of Plaintiff and Class Members. PHI and PII shall also be referred to collectively as Personal

Information. Defendants announced to the public this massive loss of information on or about February 4, 2015.

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

PARTIES

3. Plaintiff is a citizen and resident of New Hanover County, North Carolina.

4. Plaintiff is informed and believes and therefore alleges that Defendant Anthem, Inc. ("Anthem") is an Indiana Corporation headquartered in Indianapolis, Indiana. Anthem is an independent licensee of the Blue Cross and Blue Shield Association serving members in North Carolina and numerous other states and specialty plan members in other states. Plaintiff is informed and believes and therefore alleges that, through their affiliated health plans, the Anthem companies offer consumers a broad portfolio of integrated health care plans and related administrative services, together with a wide range of specialty products such as life and disability insurance benefits, dental, vision, behavioral health benefit services, as well as long term care insurance and flexible spending accounts.

5. Plaintiff is informed and believes and therefore alleges that Defendant Anthem Insurance Companies, Inc. d/b/a Anthem Blue Cross and Blue Shield ("BCBS Anthem") is an Indiana Corporation headquartered in Indianapolis, Indiana. Plaintiff is further informed and believes and therefore alleges that BCBS Anthem is an affiliate of Anthem that serves customers in the State of North Carolina, including Plaintiff Earl Edward Scofield, III.

JURISDICTION AND VENUE

6. This Court has original jurisdiction pursuant to 28 U.S.C. §1332(a)(1) and (d)(2). In the aggregate, Plaintiff's claims and the claims of the other members of the Class exceed

$5,000,000 exclusive of interest and costs. Defendants Anthem and BCBS Anthem are citizens of Indiana. Plaintiff is a citizen of North Carolina. There are numerous class members who are citizens of states other than those of the named parties hereto.

7. This Court has personal jurisdiction over Anthem because Anthem is authorized to do and does business in the State of North Carolina and in this District.

8. Venue is proper in this Court pursuant to 28 U.S.C. §1391 because many of the acts and transactions giving rise to this action occurred in this District and because Anthem is subject to personal jurisdiction in this District.

GENERAL ALLEGATIONS

9. Previously known as WellPoint, Inc., Anthem, Inc., is one of the largest for-profit managed health care companies in the United States.

10. Plaintiff has insurance issued by or through Anthem, and as a condition of providing such insurance and administering the same, Anthem has required that Plaintiff provide their PHI and PII to Anthem.

11. Anthem claims that on or about January 29, 2015, it detected a massive data breach that compromised the PHI and PII of approximately 80 million insureds.[1]

12. News of the data breach was first published by the Wall Street Journal.[2]

13. On or about February 4, 2014, Anthem began issuing statements that they had fallen victim to a data breach, stating that the "personal information from our current and former members such as their names, birthdays, medical IDs/social security numbers, street addresses,

[1] *See,* https://www.anthemfacts.com/ceo (last viewed March 3, 2015)
[2] *See,* http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720 (last viewed March 3, 2015)

email addresses and employment information, including income data" was obtained.[3]

14. On February 24, 2015, Anthem sent the following email to some of the Class members:

Anthem.

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 Mandiant, 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 AnthemFacts.com to view a list. You are receiving this

[3] *See,* https://www.anthemfacts.com/ceo (last viewed March 3, 2015)

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.

Identity Protection Services
Anthem has arranged to have AllClear ID protect your identity for two (2) years at no cost to you. The following identity protection services start on the date of this notice, or the date you previously enrolled in services based on information posted on AnthemFacts.com. You can use them at any time during the next two (2) years after your service begins.

- AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-263-7995 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition. AllClear ID maintains an A+ rating at the Better Business Bureau.
- AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of fraud against children by searching thousands of databases for use of your child's information. To use the PRO service, you will need to provide your personal information to AllClear ID. To learn more about these services, or to enroll, visit our source of truth www.AnthemFacts.com and click on the AllClear ID link from there. Please note: Additional steps may be required by you in order to activate your phone alerts.

Mailed Notification
Anthem will also individually notify potentially impacted current and former members by U.S. Postal mail with this same specific information on how to enroll in free credit monitoring and identity

protection services. These services will be provided to potentially impacted current and former members free of charge. Anthem has also established a dedicated website (AnthemFacts.com) where members can access additional information, including frequently asked questions and answers.

Toll-Free Hotline
Anthem has established a dedicated toll-free number that you can call if you have questions related to this incident. That number is 877-263-7995. We have included contact information for the three nationwide credit bureaus below.

Si necesita información en español, ingrese en antheminforma.com.

Fraud Prevention Tips
We want to make you aware of steps you may take to guard against identity theft or fraud.

We recommend that potentially impacted members remain vigilant for incidents of fraud and identity theft, including by reviewing account statements and monitoring free credit reports. In addition, you can report suspected incidents of identity theft to local law enforcement, Federal Trade Commission, or your state attorney general. To learn more, you can go to the FTC's Web site, at www.consumer.gov/idtheft, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You should be aware of scam email campaigns targeting current and former Anthem members. These scams, designed to capture personal information (known as "phishing"), are designed to appear as if they are from Anthem and the emails include a "click here" link for credit monitoring. These emails are NOT from Anthem.

- DO NOT reply to the email or reach out to the senders in any way.
- DO NOT supply any information on the website that may open, if you have clicked on a link in email.
- DO NOT open any attachments that arrive with email.

Anthem is not calling members regarding the cyber-attack and is not asking for credit card information or Social Security numbers over the phone. For more guidance on recognizing scam email, please visit the FTC Website for their article on phishing.

Credit Bureau Information

Equifax	Experian,	TransUnion
PO BOX 740241 ATLANTA GA 30374-0241 1-800-685-1111 equifax.com	PO BOX 9532 ALLEN TX 75013 1-888-397-3742 experian.com	PO BOX 6790 FULLERTON CA 92834-6790 1-800-916-8800 transunion.com

You can obtain additional information from the FTC and the nationwide credit bureaus about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit bureaus listed above. As soon as that bureau processes your fraud alert, it will notify the other two bureaus, which then must also place fraud alerts in your file. In addition, you can visit the credit bureau links below to determine if and how you may place a security freeze on your credit report to prohibit a credit bureau from releasing information from your credit report without your prior written authorization:

- Equifax security freeze: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
- Experian security freeze: http://www.experian.com/consumer/security_freeze.html
- TransUnion security freeze: http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

For Maryland and North Carolina Residents - You can obtain information from these sources about preventing identify theft:

- Visit the Federal Trade Commission website at: www.ftc.gov, or call 1-877-ID-THEFT
  or write to this address:
  Federal Trade Commission
  600 Pennsylvania Avenue NW
  Washington, DC 20580

- **Maryland:**
  Visit the Maryland Office of the Attorney General at:
  oag.state.md.us/idtheft/index.htm, or call 1-410-528-8662
  or write to this address:
  Consumer Protection Division
  Maryland Office of the Attorney General
  200 St. Paul Place
  Baltimore, MD 21202

- **North Carolina:**
  Visit the North Carolina Office of the Attorney General at:
  http://www.ncdoj.gov/Crime.aspx or call 1-919-716-6400 or
  write to this address:
  Attorney General's Office
  9001 Mail Service Center
  Raleigh, NC 27699-9001

FOR MASSACHUSSETTS RESIDENTS
Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services.

If you have been a victim of identity theft and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies listed above.

In order to request a security freeze, you will need to provide the following information:

1. **Your full name (including middle initial as well as Jr., Sr., II, III, etc.);**
2. **Social Security number;**

3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address (e.g., a current utility bill or telephone bill);
6. A legible photocopy of a government issued identification card (e.g., state driver's license or ID card or military identification);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time To remove the security freeze, you must send a written request to each of the three credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.

Worried about links?
We know you might be concerned about clicking links, so Anthem did not include any in this message. However, some email programs and smart phones automatically add links. Remember, you can always type

a web address manually in your browser instead of clicking through from this email.

This email was sent by: Anthem, Inc. 120 Monument Circle Indianapolis, IN 46204 USA

15. Anthem does not provide any information as to when its systems were compromised, how long third parties had access to its systems, or what measures have been taken to prevent further breaches.

16. Anthem does not definitively state that customers' banking and medical information was not disclosed to third parties.

17. Given Anthem's carefully worded and conclusory notices, and on information and belief, the medical information of its customers, such as claims, test results, medical history, and diagnoses were also compromised and disclosed to third parties.

18. Given Anthem's carefully worded and conclusory notices, and on information and belief, the banking and credit information of its customers was also compromised and disclosed to third parties.

19. Anthem has set up a website where the data breach was disclosed to Anthem customers by way of a letter from Joseph R. Swedish, Anthem's President and CEO. This

website also provides a short and factually vague description of the compromise.[4]

20. On information and belief, Plaintiff's PHI and PII were disclosed to third parties as a result of the data breach.

CONSEQUENCES OF DEFENDANTS' CONDUCT

21. In August 2014, the FBI warned that hackers were possibly seeking to access electronic protected health information.[5] In September, the U.S. Food and Drug Administration voiced similar worries. In January 2015, the federal government's top Health Insurance Portability and Accountability Act enforcer said that hacking of health care businesses had spiked of late. Anthem failed to take heed of these warnings and instead, recklessly and negligently allowed this catastrophic data breach, exfiltration, and disclosure to occur by its actions and omissions described herein.

22. Defendants' failure to keep Plaintiff's and class members' PHI and PII protected has resulted in severe ramifications to its customers, such as Plaintiff, which will undoubtedly continue in the months and years ahead. This cyber attack has exposed the personal information of up to 80 million customers and employees.

23. It is clear and apparent that Internet scammers have taken advantage of this massive and avoidable exposure of personal information. For example, Anthem has publically warned of a phishing ploy targeting those affected by the breach.[6] Anthem has represented to the public that it was not behind a series of emails that it seemingly sent to current and former customers, prompting recipients to click a link to access a free credit monitoring service. "These

---

[4] *See,* www.anthemfacts.com/FAQ, (last viewed March 3, 2015)
[5] *See,* http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820, (last viewed March 3, 2015)
[6] *See,* www.anthemfacts.com/FAQ, (last viewed March 3, 2015)

emails are NOT from Anthem," the company said.[7] "Anthem is not calling members regarding the cyber attack and is not asking for credit card information or Social Security numbers over the phone."[8]

24. Anthem cautioned customers to not click on any of the email's links, reply to the email, or open any attachments, even though the messages are designed to appear genuine.[9]

25. The information Defendants lost through breach and exfiltration, including Plaintiff's PHI and PII is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC").[10] Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes.[11] The FTC estimates that as many as 9 million Americans have their identities stolen each year.[12]

26. Identity thieves can use identifying data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.[13] These thieves typically do not repay such loans or charges, saddling victims with lower credit ratings, higher interest rates, collection lawsuits, and a never ending digital paper-chase to correct financial injury arising from Defendants' actions.

---

[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *See,* https://web.archive.org/web/20130117191854/http:/www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last viewed March 3, 2015)
[11] *See,* http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last viewed March 3, 2015)
[12] *See,* http://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business (last viewed March 3, 2015)
[13] *See,* http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last viewed March 3, 2015)

27. Identity thieves can use PHI and PII, such as that belonging to the Class, which Defendants failed to keep secure, to perpetrate a variety of crimes that include both financial loss and other types of harm and injury to the victims. For example, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

28. In addition, identity thieves may procure medical services using the Plaintiff's PHI and PII or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. These illegal activities can result in money judgments and even imprisonment for identity theft victims.

29. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts . . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[14]

30. Researchers have concluded:

---

[14] *See, The President's Identity Theft Task Force Report: Combating Identity Theft, A Strategic Plan,* at p.11 (Apr. 2007), available at http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last viewed March 3, 2015).

> In addition to the financial harm associated with other types of identity theft, victims of medical identity theft may have their health and life endangered by inaccurate entries in their medical records. Inaccurate information . . . can potentially cause victims to receive improper medical care, have [their] insurance depleted, become ineligible for health or life insurance, or become disqualified from some jobs. [Victims] may not even be aware that a theft has occurred because medical identity theft can be difficult to discover. Few consumers regularly review their medical records, and victims may not realize that they have been victimized until they receive collection notices, or they attempt to seek medical care themselves, only to discover that they have reached their coverage limits. . . .
>
> With the advent of the prescription drug benefit of Medicare Part D, the Department of Health and Human Services' Office of the Inspector General (HHS OIG) has noted a growing incidence of health care frauds involving identity theft. [Identity thieves can] use [such information] fraudulently to enroll unwilling beneficiaries in alternate Part D plans in order to increase their sales commissions. The types of fraud that can be perpetrated by an identity thief are limited only by the ingenuity and resources of the criminal.[15]

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

> [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.[16]

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

> [A] new number probably will not solve all your problems. This is because other

[15] MARK A. PRIGANC, IDENTITY THEFT: THE PERSONAL GUIDE 32-33 (2008).
[16] GAO, *Report to Congressional Requesters,* at p.29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf, (last viewed March 3, 2015).

> governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other personal information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[17]

33. Plaintiff and the Class he seeks to represent now face years of constant surveillance of their financial and medical records, credit rating impairment, monitoring, loss of rights, and potential medical problems.

PLAINTIFF'S FACTUAL ALLEGATIONS

34. Plaintiff Earl Edward Scofield, III, is a customer of Defendants. Plaintiff is a flight attendant for U.S. Airways (now American Airlines) and received his health insurance as an employment benefit through his employer. This health insurance is either issued by Anthem and/or procured through Anthem and/or administered by Anthem as a third-party Administrator. During the course of his procurement of insurance and the administration thereof, he was required to provide Defendants with sensitive personal and financial information, including PII and PHI. At all relevant times hereto, Anthem has provided on-line assurances of PHI and PII protection and security to its customers:

---

[17] SSA, *Identity Theft and Your Social Security Number*, at p. 7-8, SSA Publication No. 05-10064 (Dec. 2013), available at http://www.ssa.gov/pubs/10064.html, (last viewed March 3, 2015).

Personal Information (Including Social Security Number) Privacy Protection Policy

Anthem Blue Cross maintains policies that protect the confidentiality of personal information, including Social Security numbers, obtained from its members and associates in the course of its regular business functions. Anthem Blue Cross is committed to protecting information about its customers and associates, especially the confidential nature of their personal information (PI).

Personal Information is information that is capable of being associated with an individual through one or more identifiers including but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number, and does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

Anthem Blue Cross is committed to protecting the confidentiality of Social Security numbers and other Personal Information.

Anthem Blue Cross's Privacy Policy imposes a number of standards to:

- guard the confidentiality of Social Security numbers and other personal information,
- prohibit the unlawful disclosure of Social Security numbers, and
- limit access to Social Security numbers.

***

Anthem Blue Cross safeguards Social Security numbers and other personal information by having physical, technical, and administrative safeguards in place.[18]

35. Plaintiff had every right to believe and place reliance on Defendants' assurance that they would maintain his PII and PHI in a secure manner and provided the same to Defendants in reliance on those assurances. Had Plaintiff known that Defendants would not maintain his PII and PHI in a reasonably secure manner, he would never have provided that information to Defendants and would never have procured and paid for insurance issued by or through the Defendants or administered by the Defendants.

[18] *See,* https://www.anthem.com/ca/health-insurance/about-us/privacy (last viewed March 3, 2015)

36. On February 17, 2015, Plaintiff received an email from the Association of Professional Flight Attendants, a union with whom Plaintiff is a member. This email was the first notice of the breach that Plaintiff received. The Union's email stated:

> Anthem security breach impacting US Airways employees
>
> Anthem, our administrator for legacy US Airways healthcare plans, was recently the target of a very sophisticated external cyber attack. Current and former Anthem members dating back to 2004 are being offered identity repair assistance and credit monitoring services via anthemfacts.com. Additionally, members of Blue Cross and Blue Shield companies (including BCBS of Texas) who used their Blue Cross and Blue Shield insurance in one of fourteen states where Anthem, Inc. operates may be impacted and are also eligible. These states include California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Nevada, New Hampshire, New York, Virginia, and Wisconsin....

37. Defendants have informed the public that they will issue a written notification to customers whose PII has been compromised in the data breach. To date, Plaintiff has never been notified directly in writing by the Defendants that his PHI and PII were compromised.

38. In fact, Plaintiff 's PII and PHI have been stolen and otherwise compromised as a result of this massive data breach.

39. On or about January 29, 2015, Plaintiff had his 2014 tax return prepared by H&R Block in Wilmington North Carolina. When H&R Block attempted to electronically file the 2014 tax return, the filing was rejected because someone else had already filed a tax return under his name with his social security number.

40. Plaintiff has been forced to expend funds with tax preparers as a result of this previous tax filing that has denied him the ability to receive his tax refund. Plaintiff paid his tax preparers $417.50 and cannot wait to have these funds taken from his tax return as is normally the case. Once again, Plaintiff, at the very least, has lost the time value of his money. If he is unable to obtain his tax refund, then he will lose these funds altogether.

41. Among other things, as a response to this theft, Plaintiff has:

a. Contacted the Internal Revenue Service Identity Protection Specialized Unit and reported the theft;

b. Reported the theft to the Wilmington, North Carolina police department;

c. Prepared and filed a Department of Treasury –Internal Revenue Service Form 14039, tiled "Identify Theft Affidavit";

d. Contacted credit bureaus and placed a "fraud alert" on his file;

e. Contacted the Social Security Administration's fraud hotline;

f. Ordered a copy of his Personal Earnings and Benefits Estimate (PEBS) from the Social Security Administration; and

g. Ordered Credit reports.

42. Plaintiff's social security number was stolen as a result of the breach, and the thieves have either filed the fraudulent tax return themselves or sold his information to others who perpetrated the crime.

43. As a direct and proximate result of the data breach, Plaintiff has not been able to receive his tax refund. Plaintiff has been informed by Internal Revenue representatives that this tax refund will not be received for many months and possibly years. In addition, Plaintiff has been informed by these representatives that the identity theft will impact his 2015 filing.

44. Plaintiff is losing the time value of his tax refund and is incurring costs to obtain his money, the theft of which was caused by the data breach. Further, Plaintiff has been harmed by having his personal data disclosed to those who obviously intend to use the data to his financial detriment.

45. Plaintiff's PII and PHI have significant value to sophisticated criminals, who are

willing to pay to purchase this stolen information. In addition to the theft that has already occurred, he faces the imminent threat of future additional harm from the increased risk of identity theft and fraud due to his PII and PHI being used in nefarious ways by those who have stolen the information or those who may purchase the information on the Internet black market.

CLASS ACTION ALLEGATIONS

46. Plaintiff brings this action on his behalf, and on behalf of all other persons similarly situated ("the Class"). The Class that Plaintiff seeks to represent is:

> All persons who reside in North Carolina and have purchased health insurance from Anthem, Inc., and BCBS Anthem or purchased insurance where Anthem acted as an Administrator and whose personal and/or financial information was breached as a result of the data breach announced on or about February 5, 2015.
>
> Excluded from the Class are Defendants; officers, directors, and employees of Defendants; any entity in which Defendants have a controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of the Defendants, and all judges to whom the case is assigned, and the members of their respective staff.

47. The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, it is well in excess of one hundred thousand.

48. There is a well-defined community of interest among the members of the Class because common questions of law and fact predominate, Plaintiff's claims are typical of the members of the Class, and Plaintiff can fairly and adequately represent the interests of the Class.

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

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

b. Whether Anthem unreasonably delayed in notifying affected customers of the data breach;

c. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach;

d. Whether Defendants' conduct was negligent;

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

f. Whether Plaintiff and the Class are entitled to damages and/or injunctive relief.

50. Plaintiff's claims are typical of those of other Class members because Plaintiff's PHI and PII, like that of every other class member, were misused and/or disclosed by Defendants.

51. Plaintiff will fairly and accurately represent the interests of the Class.

52. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which would establish incompatible standards of conduct for Defendants and would lead to repetitive adjudication of common questions of law and fact. Accordingly, class treatment is superior to any other method for adjudicating the controversy. Plaintiff knows of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action under Rule 23(b)(3).

53. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' violations of law

inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

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

55. Plaintiff seeks the award of actual damages on behalf of the Class.

COUNT I
(Negligence)

56. Plaintiff repeats and realleges all factual allegations set forth in this Complaint as if fully set forth herein.

57. Upon accepting and storing Plaintiff's and Class Members' PHI and PII in its respective computer database systems, Defendants undertook and owed an affirmative duty to Plaintiff and Class Members to exercise reasonable care. It was Defendants' obligation to secure and safeguard that information and to utilize commercially reasonable methods to do so. Defendants knew that the PII and PHI were private and confidential and should be protected as private and confidential. A duty to maintain and protect this information also arose by operation of law, including the obligations imposed by HIPAA.

58. Defendants breached their duties to Plaintiff and Class Members to adequately protect and safeguard this information by knowingly disregarding standard principles relating to the securing of PHI and PII. Defendants negligently failed to provide adequate supervision and oversight of the PHI and PII which were, and are, entrusted to it, in spite of the known risks and foreseeable likelihood of breach and misuse. Defendants' failures permitted third persons to gather Plaintiff's and Class Members' PHI and PII, misuse the PHI and PII, and intentionally disclose it to others without consent.

59. The law also imposes an affirmative duty on Defendants to timely disclose the theft of the PHI and PII so that Plaintiff and Class Members could be vigilant in attempting to determine if any of their accounts or assets had been stolen through identity theft.

60. Defendants breached their duties to notify Class Members of the unauthorized access by waiting many months after learning of the breach to provide such notice. To date, Defendants have still not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access.

61. Through Defendants' acts and omissions described in this Complaint, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and Class Members' PHI and PII during the time it was within Defendants' possession or control.

62. Further, through its failure to provide timely and clear notification of the data breach to consumers, Defendants negligently prevented Plaintiff and Class Members from taking meaningful, proactive steps to investigate possible identity theft.

63. Defendants improperly and inadequately safeguarded the PHI and PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access.

64. Given the extensive publicity about the efforts of criminal enterprises to obtain PHI and PII and its history of employees improperly accessing and exploiting the PHI and PII of patients, it was foreseeable to Defendants that the Plaintiff's and Class Members' PHI and PII in their possession might be attractive to misappropriation and misuse.

65. In fact, Plaintiff's PII has been misused as set forth above. Plaintiff has been damaged by reason of this theft and has incurred and will continue to incur damages related to the fraudulent tax return that was filed with his social security number.

66. For all the reasons stated above, Defendants' conduct was negligent and departed from reasonable standards of care including, but not limited to: failing to adequately protect the PHI and PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiff and Class Members' PHI and PII; and failing to provide Plaintiff and Class Members with timely and sufficient notice that their sensitive PHI and PII had been compromised.

67. Neither Plaintiff nor the other Class Members contributed to the data breach or subsequent misuse of their PHI and PII as described in this Complaint.

68. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and every member of the Class has been put at risk of identity theft and has an obligation to mitigate damages through credit monitoring services. Defendants are liable to each and every member of the Class for the reasonable costs of future credit monitoring services. Defendants are also liable to those Class Members, including Plaintiff, who have directly sustained damages as a result of their identity theft.

COUNT II
(Breach of Fiduciary Duty)

69. Plaintiff repeats and realleges all factual allegation set forth in this Complaint as if fully set forth herein.

70. As Defendants required Plaintiff and the Class members to provide sensitive PII and PHI as part of their business of providing insurance and administration of insurance to Plaintiff and the Class, the Defendants were placed in a position of trust and confidence with the

Plaintiff and the Class. As such, Plaintiff and Class Members have a special relationship with Defendants, and Defendants owed a fiduciary duty to Plaintiff and Class Members to keep their PHI and PII private and confidential and to protect it from misuse by others.

71. Defendants breached the fiduciary duty it owed to Plaintiff and Class Members by failing to adequately safeguard their PHI and PII against unauthorized disclosure and misuse.

72. Defendants further breached the fiduciary duties it owed to Plaintiff and Class Members by failing to timely notify them of the breach of their PHI and PII.

73. Defendants' failure to adequately safeguard Plaintiff' and Class Members' PHI and PII has resulted in losses and damages to Plaintiff and members of the Class.

COUNT III
(Breach of Contract and Implied Contract)

74. Plaintiff repeats and realleges all factual allegation set forth in this Complaint as if fully set forth herein.

75. When Plaintiff became an insured of Defendants', there arose a contract between the Plaintiff and Defendants. The same is true with respect to the contractual relationship that arose between Defendants and every other member of the Class.

76. Anthem's contract assures customers that they are committed to protecting the confidentiality of personal information, including social security numbers, and that they have numerous safeguards in place to protect such information.

77. In exchange for compensation that was to be paid by Plaintiff and by the Class, Defendants were to provide health insurance and/or administration of the same.

78. Expressly or implicitly in the agreement made by Defendants was an understanding that, as part of the health insurance and administration to be provided to Plaintiff

and members of the Class, Defendants would protect the sensitive information provided by Plaintiff and the Class, as required by accepted law and the standards in Defendants' businesses.

79. Defendants breached their express or implied agreement, causing damages to Plaintiff and members of the Class for which recovery should be made as demanded hereafter.

COUNT IV
(Negligent Misrepresentation)

80. Plaintiff repeats and realleges all factual allegation set forth in this Complaint as if fully set forth herein.

81. Defendants, by their actions alleged herein, negligently supplied false information to Plaintiff and Class Members regarding Defendants' safeguarding of Plaintiff's and Class Members' Social Security numbers and other personal information by having physical, technical, and administrative safeguards in place.

82. Plaintiff and Class Members are foreseeable persons under North Carolina law.

83. Plaintiff and Class Members reasonably relied on such false information.

84. Plaintiff and Class Members suffered economic injury proximately resulting from such reliance.

85. As a result of Defendants' actions alleged herein, Plaintiff and the Class are entitled to all remedies at law or in equity under North Carolina law.

COUNT V
(Unjust Enrichment)

86. Plaintiff repeats and realleges the factual allegation set forth in this Complaint as if fully set forth herein.

87. Plaintiff and Class Members conferred a monetary benefit on Defendants in the form of monies paid for goods and services.

88. Defendants appreciate and have knowledge of the benefits conferred upon it by Plaintiff and the Class and accepted the same.

89. The monies that Plaintiff and the Class paid to Defendants were supposed to be used by Defendants, in part, to pay for the costs of data management and security that would, in part, protect customers' privacy and prevent disclosure of customers' PII and PHI.

90. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and the other members of the Class because Defendants failed to implement data management and security measures that Plaintiff and the Class Members paid for and that are otherwise mandated.

91. As a result of Defendants' conduct, Plaintiff and the other members of the Class suffered damages in the amount of the difference between the price they paid for Defendants' insurance and administration services as promised and the actual diminished value of its insurance and administration services.

COUNT VI
(UNFAIR AND DECEPTIVE TRADE PRACTICES
N.C. GEN. STAT. § 75-1, *et seq.*)

92. Plaintiff repeats and realleges the factual allegations set forth in this Complaint as if fully set forth herein.

93. The North Carolina Unfair and Deceptive Trade Practices Act (hereinafter "UDTPA") is expressly intended to protect "consumers" like Plaintiff and Class Members from unfair or deceptive trade practices.

94. Plaintiff and Class Members have a vested interest in the privacy, security, and integrity of their PII and PHI; therefore, this interest is a "thing of value" as contemplated by the UDTPA.

95. Defendants are a "person" within the meaning of the UDTPA and, at all pertinent times, were subject to the requirements and proscriptions of the UDTPA with respect to all of their business and trade practices described herein.

96. Plaintiff and Class Members are "consumers" and are "likely to be damaged" by Defendants' ongoing deceptive trade practices.

97. Defendants engaged in unfair and deceptive trade practices when they accepted their customers' PII and PHI and failed to adequately safeguard them.

98. Defendants violated the UDTPA by failing to properly implement adequate, commercially reasonable security measures to protect consumers' sensitive PII and PHI.

99. By failing to disclose that they do not enlist industry standard security practices, which renders Defendants' insurance and administration services particularly vulnerable to data breaches, Defendants engaged in a fraudulent business practice that is likely to deceive a reasonable consumer.

100. A reasonable consumer would not have purchased insurance from Defendants or purchased insurance administered by Defendants had he or she known the truth about Defendants' security procedures. By withholding material information about Defendants' security practices, Defendants were able to convince customers to provide and entrust their PII and PHI to Defendants. Had the Class Members, as reasonable persons, known the truth about Defendants' security procedures, they would not have purchased insurance from Defendants or purchased insurance administered by Defendants.

101. Defendants' failure to disclose that they do not enlist industry standard security practices also constitutes an unfair business practice under the UDTPA. Defendants' conduct is unethical, unscrupulous, and substantially injurious to Plaintiffs and the Class. Whereas

Defendants' competitors have spent the time and money necessary to appropriately safeguard customer information, Defendants have not—to the detriment of their customers and to competition.

102. Defendants also violated the UDTPA by failing to immediately notify the affected Plaintiff and Class Members of the nature and extent of the data breach.

103. Further, Defendants violated the UDTPA by violating North Carolina's Identity Theft Protection Act (ITPA), N.C.G.S. § 75-60, *et. seq*. (ITPA).

104. Defendants violated ITPA by:

a. Failing to prevent the PHI and PII of customers from falling into unauthorized hands; and

b. Failing to provide adequate notice of the security breach to affected consumers upon discovery that their system had been compromised and PII and PHI had been stolen.

105. Plaintiff and Class Members have suffered ascertainable losses as a direct result of Defendants' employment of unconscionable acts or practices and unfair or deceptive acts or practices.

106. At all material times, Defendants' deceptive trade practices were willful within the meaning of the UDTPA, and, accordingly, Plaintiff and the Class are entitled to an award of attorneys' fees, costs, and other recoverable expenses of litigation.

107. Under the UDPTA, Plaintiff and the Class are entitled to preliminary and permanent injunctive relief without proof of monetary damages, loss of profits, or intent to deceive. Plaintiff and the Class seek equitable relief and seek to enjoin Defendants on terms that the Court considers appropriate.

108. Defendants' conduct caused and continues to cause substantial injury to Plaintiff and Class Members. Unless preliminary and permanent injunctive relief is granted,

a. Plaintiff and the Class will suffer harm;

b. Plaintiff and the Class Members do not have an adequate remedy at law; and

c. the balance of the equities weighs in favor of Plaintiff and the Class.

109. Plaintiff accordingly requests that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures, including, but not limited to, ordering that:

a. Defendants utilize strong industry standard encryption algorithms for encryption keys that provide access to stored customer data;

b. Defendants implement the use of their encryption keys in accordance with industry standards;

c. Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

d. Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring;

e. Defendants audit, test, and train their security personnel regarding any new or modified procedures;

f. Defendants, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if

one area of Defendants is compromised, hackers cannot gain access to other portions of Defendants' systems;

g. Defendants purge, delete, and destroy in a reasonable secure manner customer data not necessary for its provisions of services;

h. Defendants, consistent with industry standard practices, conduct regular database scanning and security checks;

i. Defendants, consistent with industry standard practices, evaluate web applications for vulnerabilities to prevent web application threats to consumers who purchase Defendants' insurance and insurance administered by Defendants' services through the Internet;

j. Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

k. Defendants meaningfully educate their customers about the threats the customers face as a result of the loss of their PHI and PII to third parties, as well as the steps Defendants' customers must take to protect themselves.

110. Plaintiff further requests that the Court require Defendants to identify and notify all members of the Class who have not yet been informed of the Security Breach, and to notify affected customers of any future data breaches by email within 24 hours of Defendants' discovery of a breach or possible breach and by mail within 72 hours.

111. As a result of Defendants' violations of the UDPTA, Plaintiffs and Class Members have suffered injury in fact and lost money or property, as detailed in this Complaint.

They purchased products or services they otherwise would not have purchased or paid more for those products and services than they otherwise would have paid. Plaintiff requests that the Court issue sufficient equitable relief to restore Plaintiff and Class Members to the positions they would have been in had Defendants not engaged in unfair or deceptive trade practices, including by ordering restitution of all funds that Defendants may have acquired as a result of its unfair or deceptive trade practices.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiff and Class Members;

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

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

E. For an award of punitive damages;

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

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial of his claims to the extent authorized by law.

Dated: March 5, 2015

Respectfully submitted,

/s/ Joel R. Rhine
Joel R. Rhine
RHINE LAW FIRM, P.C.
1612 Military Cutoff Road, Suite 300
Wilmington, NC 28403
Tel: (910) 772-9960
Fax: (910) 772-9062
Email: jrr@rhinelawfirm.com
North Carolina State Bar No. 16028

MORGAN & MORGAN COMPLEX LITIGATION GROUP
John A. Yanchunis*
jyanchunis@forthepeople.com
Florida State Bar No. _____
Rachel Soffin*
rsoffin@forthepeople.com
Florida State Bar No. _____
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
Fax: (813) 222-2434

ABBOTT LAW GROUP P.A.
Steven W. Teppler*
steppler@abbottlawpa.com
Florida State Bar No. _____
F. Catfish Abbott*
fabbott@abottlawpa.com
Florida State Bar No. _____
2929 Plummer Cove Road
Jacksonville, FL 32223
Tel: (904) 292.1111
Fax: (904) 292-1200
Attorneys for Plaintiff and the Proposed Class

****To Be Admitted Pro Hac Vice***