UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF INDIANA

2015 FEB 20 PM 4: 37

LAURA A, BRIGGS

FRANCINE BLAIN, NICHOLAS KALFA, CORINNE BERNSTEIN and FREDA BEIN MULDOON on behalf of themselves and all others similarly situated,

Plaintiffs,

VS.

ANTHEM, INC.,

Case No.

JURY TRIAL DEMANDED

15-w-0288 RLY-MJD

Defendant.

CLASS ACTION COMPLAINT

Plaintiffs Francine Blain, Nicholas Kalfa, Corinne Bernstein and Freda Bein Muldoon, on behalf of themselves and all other persons similarly situated, allege the following claims against Anthem, Inc. ("Anthem" or the "Company") based upon personal knowledge with respect to themselves and their own acts and upon information and belief as to all other matters derived from, among other things, the investigation of counsel, including review of publicly available documents and information.

SUMMARY OF THE ACTION

1. On February 4, 2015, Anthem in a letter to members posted on the Anthem website, confirmed that the security of an Anthem database containing extremely sensitive personal identifying information ("PII"), including the names, dates of birth, member ID/social security numbers, addresses, phone numbers, email addresses and employment information of approximately 80 million individuals including customers, former customers and their children

("Insureds") was breached by unidentified hackers. The Insureds' PII that Anthem lost to hackers contained everything a criminal needs to engage in identity theft.

- 2. Anthem's investigation of the breach is ongoing and the full extent of the PII accessed and taken by the hackers has yet to be disclosed.
- 3. On February 5, 2015, U.S. Senator Richard Blumenthal stated to the Senate Commerce Committee that the Anthem data breach "is not only breathtaking in its scope and scale, it is potentially heartbreaking and life changing for the tens of millions [] affected . . . These attacks are real and they hurt real people and companies [] collecting sensitive consumer data had an obligation to do more to protect that information."
- 4. On its website, <u>www.anthemfacts.com</u>, Anthem warns Insureds to take steps to protect themselves from the imminent consequences of the data breach and of the need to be vigilant in monitoring their financial and insurance information. Anthem's chief information officer, Thomas Miller, is quoted as stating on the Anthem website, "At least you know that this compromise has happened . . . We will let you know as soon as we know more."
- 5. On February 7, 2015, cyber security expert Neil O'Farrell was quoted by the *Indianapolis Star* as stating "This is absolutely the worst kind of data breach, because thieves have stolen the information that's the most valuable, the most dangerous and impossible to change or cancel . . . This is a mass victimization of the worst kind." According to experts, the type of information the hackers accessed (the "keys to the kingdom" to commit any kind of identity theft) could create problems for those affected for years to come and not just individuals, but entire families.
- 6. Plaintiffs Blain, Kalfa, Bernstein and Muldoon each entrusted their PII with Anthem and rightfully expected Anthem to protect and safeguard that information from outsiders. Yet, Anthem failed to do so. Despite the Company's prior data security lapses and

repeated warnings to take steps to protect its Insureds' PII from hackers, the sensitive PII of the tens of millions of Anthem Insureds taken in the data breach was not even encrypted on the Company's database. According to Trent Telford, a security expert quoted in the February 9, 2015 *The Los Angeles Times*, it was "irresponsible for [Anthem] not to encrypt the data."

- 7. Sensitive PII was not segregated and was not stored in such a way to prevent whole files of the entire Company being accessible (it appears that *all Anthem product lines are impacted*) and then exported from Anthem's computer system to computers controlled by the hackers outside of Anthem.
- 8. Passwords that provided access to the Anthem computer system were not sufficiently robust. Access to high-level Anthem computer administrator accounts was not adequately controlled or monitored.
- 9. Therefore, Plaintiffs Blain, Kalfa, Bernstein and Muldoon bring this action, on behalf of themselves and all other persons who entrusted their PII to Anthem which Anthem did not keep in a sufficiently secure manner resulting in improper access to hackers who took such information as announced on February 4, 2015 (the national "Class"), as well as a sub-class of California residents with respect to Counts VI-VIII (the "California Sub-Class"); a sub-class of New York residents with respect to Count IX (the "New York Sub-Class"), a sub-class of New Jersey residents with respect to Count X (the "New Jersey Sub-Class"), and a sub-class of New Hampshire residents with respect to Counts XI-XII (the "New Hampshire Sub-Class"), to recover for the harm caused to them and the other members of the Class and Sub-Classes by Defendant Anthem. The precise dates the Anthem breach began or ended is not known at this time.

THE PARTIES

- 10. Plaintiff Francine Blain is a resident of the state of California and had a health insurance policy written by Defendant Anthem in California during the time of the breach alleged herein.
- 11. Plaintiff Nicholas Kalfa is a resident of the state of New York and had a health insurance policy written by Empire Blue Cross, Blue Shield ("BCBS") during the time of the breach alleged herein.
- 12. Plaintiff Corinne Bernstein is a resident of the state of New Jersey and had a health insurance policy written by Blue Cross, Blue Shield of Anthem Health Plans of Virginia, Inc.
- 13. Plaintiff Freda Bein Muldoon is a resident of the state of New Hampshire and had secondary health insurance coverage by Anthem under the Federal Employee Health Benefits Program though Blue Cross & Blue Shield during the time of the breach alleged herein.
- 14. Defendant Anthem Inc., formerly known as Wellpoint, Inc., is incorporated under the laws of the state of Indiana and maintains its principal executive offices at 120 Monument Circle, Indianapolis, Indiana 46204. According to its filings with the Securities and Exchange Commission, Anthem is one of the largest health benefits companies in terms of medical membership in the United States, serving approximately 37.5 million medical members through its affiliated health plans and approximately 68.5 million individuals through its subsidiaries as of September 14, 2014. Anthem offers a broad spectrum of network-based managed care plans to large and small employers, individual, Medicaid and Medicare markets. Anthem is an independent licensee of the Blue Cross and Blue Shield Association, or BCBSA, an association of independent health benefit plans. Anthem serves its members as the Blue Cross licensee for California and as the Blue Cross and Blue Shield, or BCBS, licensee for Colorado, Connecticut,

Georgia, Indiana, Kentucky, Maine, Missouri (excluding 30 counties in the Kansas City area), Nevada, New Hampshire, New York (as BCBS in 10 New York City metropolitan and surrounding counties, and as Blue Cross or BCBS in selected upstate counties only), Ohio, Virginia (excluding the Northern Virginia suburbs of Washington, D.C.), and Wisconsin. In a majority of these service areas Anthem does business as Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, and Empire Blue Cross Blue Shield, or Empire Blue Cross (in its New York service areas). Anthem also conducts business through its Amerigroup Corporation, or Amerigroup subsidiary in Florida, Georgia, Kansas, Kentucky, Louisiana, Maryland, Nevada, New Jersey, New Mexico, New York, Tennessee, Texas and Washington. Anthem also serves customers throughout the country as Health Link, UniCare, and in certain Arizona, California, Nevada, New York and Virginia markets, through its CareMore Health Group, Inc., or CareMore, subsidiary. Anthem is licensed to conduct insurance operations in all 50 states through its subsidiaries.

JURISDICTION AND VENUE

- 15. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d)(2). The amount in controversy exceeds \$5,000,000 exclusive of interest and costs. Plaintiffs and Defendant are citizens of different states. There are more than 100 members in the alleged national Class and the Sub-Classes.
- 16. This Court has jurisdiction over Anthem, Inc., because Anthem maintains its principal place of business in Indianapolis, Indiana, is incorporated under the laws of Indiana, regularly conducts business in Indiana and has sufficient minimum contacts in Indiana. Anthem intentionally avails itself of this jurisdiction by marketing and selling products from Indiana to millions of consumers nationwide, including insureds in Indiana.

CLASS ACTION ALLEGATIONS

- 17. Plaintiffs bring this class action pursuant to the Federal Rules of Civil Procedure 23(a) and (b)(3), on behalf of themselves and all others similarly situated, consisting of all persons in the United States, the national Class, and on behalf of residents of California, New York, New Jersey and New Hampshire Sub-Classes with respect to Counts VI-XII herein, who have had their PII improperly accessed and taken due to Anthem's data breach and were damaged thereby herein, respectively. The Class and Sub-Classes do not include the officers or directors of the Defendant.
- 18. The Class and Sub-Classes consist of millions of Anthem Insureds throughout the United States, California, New York, New Jersey and New Hampshire. While the exact number of members of the Class and Sub-Classes and the identities of individual members of the Class and Sub-Classes are unknown at this time, and can only be ascertained through appropriate discovery, based on the fact that millions of Insureds have been affected, the Class and Sub-Classes are each so numerous that joinder of all members is impracticable.
- 19. Anthem's conduct affected all members of the Class and Sub-Classes in exactly the same way. The Defendant's failure to properly safeguard its Insureds' PII is completely uniform among the Class and Sub-Classes.
- 20. Questions of law and fact common to all members of the Class and Sub-Classes predominate over any questions affecting only individual members. Such questions of law and fact common to the Class and Sub-Classes include:
 - a. whether the Defendant acted wrongfully by failing to properly safeguard its Insureds' PII;
 - b. whether Defendant's conduct violated law;
 - c. whether the Plaintiffs and the other members of the Class and Sub-Classes have been damaged, and, if so, what is the appropriate relief; and

- d. whether the Defendant breached implied contracts with members of the Class and Sub-Classes by failing to properly safeguard their PII.
- 21. The Plaintiffs' claims, as described herein, are typical of the claims of all other members of the Class and Sub-Classes, as the claims of the Plaintiffs and all other members of the Class and Sub-Class members arise from the same set of facts regarding the Defendant's failure to protect the members of the Class and Sub-Classes' PII. The Plaintiffs maintain no interests antagonistic to the interests of other members of the Class and Sub-Classes.
- 22. The Plaintiffs are committed to the vigorous prosecution of this action and have retained competent counsel experienced in the prosecution of class actions of this type.

 Accordingly, the Plaintiffs are adequate representatives of the Class and Sub-Classes and will fairly and adequately protect the interests of the Class and Sub-Classes.
- 23. This class action is a fair and efficient method of adjudicating the claim of the Plaintiffs and the Class and Sub-Classes for the following reasons:
 - a. common questions of law and fact predominate over any question affecting any individual Class or Sub-Class members;
 - b. the prosecution of separate actions by individual members of the Class and Sub-Classes would likely create a risk of inconsistent or varying adjudications with respect to individual members of the Class and Sub-Classes thereby establishing incompatible standards of conduct for Defendant or would allow some members of the Class or Sub-Classes' claims to adversely affect other members of the Class or Sub-Classes' ability to protect their interests;
 - c. this forum is appropriate for litigation of this action since a substantial portion of the transactions, acts, events, and omissions alleged herein occurred in this District;
 - d. the Plaintiffs anticipate no difficulty in the management of this litigation as a class action; and
 - e. the Class and Sub-Classes are readily definable, and prosecution as a class action will eliminate the possibility of repetitious litigation, while also providing redress for claims that may be too small to support the expense of individual, complex litigation.

24. For these reasons, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

SUBSTANTIVE ALLEGATIONS

- 25. On February 4, 2015, Anthem announced a severe data breach of its computer network that may impact more than 80 million individuals nationwide.
 - 26. The Company's website, <u>www.anthemfacts.com</u>, further revealed that:

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.

27. In terms of the Insureds' sensitive PII that was improperly accessed and exported from the Anthem computer network, www.anthemfacts.com states:

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.

28. The Anthem website revealed the massive scope of the breach:

At this point in the investigation, it appears that all product lines are impacted except for those current or former Anthem members who had coverage for workers compensation insurance only.

* * *

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 and HealthLink.

(emphasis added).

29. The Anthem website states that individual Insureds whose sensitive PII stored on Anthem's computer system was accessed improperly will, at some point in the future, be personally notified via U.S. Mail:

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

(emphasis added).

30. On February 5, 2015, the State of California Insurance Commission issued a press release which quoted Insurance Commissioner Dave Jones as stating:

Health insurers have not only consumers' financial information but also sensitive medical information. Although early reports from Anthem indicate that medical information was not breached, the information reportedly taken does open the door to identity theft and fraud against tens of millions of consumers. The Anthem breach underscores the need for insurance companies to take every precaution to protect their customers' information and make their consumers whole when a data breach occurs.

- 31. On February 6, 2015, *The Los Angeles Times*, at latimes.com reported that the U.S. Department of Health and Human Services, the agency that enforces the Health Insurance Portability and Accountability Act ("HIPAA") is looking into the Anthem data breach. According to the latimes.com, Federal officials said the names, Social Security numbers and other personal information of health plan members is protected under HIPAA regardless of whether treatment of medical diagnoses are disclosed.
- 32. Anthem has claimed and continues to claim that the Insureds' PII will be protected. The Company website contains a Personal Information (Including Social Security Number) Privacy Protection Policy that states:

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 . . .

https://www.anthem.com/ca/health-insurance/about-us/privacy#web

- 33. Despite its stated policies, the Company has experienced several lapses in security of sensitive data of its customers.
- 34. The Associated Press reported on February 5, 2015 that in 2013, federal regulators pointed out computer vulnerabilities at Anthem in a breach involving information on more than 600,000 customers and that Anthem paid \$1.7 million to resolve the matter.

 According to the Associated Press, the U.S. Department of Health and Human Services said that security weaknesses left names, birthdays, addresses, telephone numbers, Social Security numbers, and health data accessible to unauthorized users. The regulator also stated that Anthem didn't have adequate policies for authorizing access, didn't perform a needed technical evaluation after a software upgrade, and did not have technical safeguards to verify that the people or entities seeking access were authorized to view information on the system.
- 35. In 2008, according to the Associated Press, Anthem offered free credit monitoring after personal information for about 128,000 customers in several states had been exposed online. And in 2006, computer tapes containing personal information of 200,000 Anthem members were stolen in Massachusetts.

Warnings Leading Up To Breach

- 36. Anthem must have been aware of the ominous red flags raised by high-profile intrusions and data theft by hackers of computer systems of large U.S. retailers such as Target, Staples, and Home Depot and financial institutions such as JP Morgan, and the necessity of securing customer information stored on Anthem computers.
- 37. And there were numerous warnings directed specifically to health care companies. For example, in April 2014, the FBI issued a warning directly to the health care industry that lax security rendered health care companies prime targets for data thieves.

- 38. On April 27, 2014, *Reuters* reported that the FBI has warned healthcare providers their cybersecurity systems are lax compared to other sectors, making them vulnerable to attacks by hackers searching for Americans' personal medical records and health insurance data and that health data is far more valuable to hackers on the black market than credit card numbers because it tends to contain details that can be used to access bank accounts or obtain prescriptions for controlled substances. *Reuters* reported that a series of privately commissioned reports published over the past few years have urged healthcare systems to boost security.
 - 39. In fact, the FBI warning dated April 4, 2014 quoted by *Reuters* states: The healthcare industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely.
- 40. Anthem, nevertheless, failed to take necessary steps to protect its Insureds' PII stored on its computer system. Among other things, the tens of millions of records that contained sensitive PII of the Plaintiffs and other members of the Class and Sub-Classes were not encrypted. Encryption is the process of encoding information in such a way that only authorized parties can read it. Properly encrypted records would have been useless to hackers.

The 2015 Data Breach

41. According to the February 4, 2015 *The Wall Street Journal*, Anthem discovered the data breach during the last week of January 2015 when an Anthem systems administrator noticed that a database query was being run using his identifier code although he had not initiated the query. In other words, the administrator's computer ID was used to operate Anthem's computer system by an unknown and unauthorized person to collect and export PII to a computer outside the Anthem system. Anthem chief information officer, Thomas Miller, said that investigators tracked Anthem's hacked data to a web-storage service outside Anthem and were able to freeze the hacked data there. What is not known is how much of the hacked data

the hackers copied and moved to still another unknown location by the time it was found by investigators at the web-storage site.

42. Anthem has not revealed how its computer system was breached, who is responsible for the breach and or how many Insureds' PIIs were affected. Anthem's website says it appears that all product lines are impacted except for those current or former Anthem members who had coverage for workers compensation insurance only. The database that was breached contained the personal records of about 80 million individuals.

Plaintiffs and Members of the Class and Sub-Classes Have Been Harmed

43. The scams which the Anthem data breach will subject upon the Class and Sub-Classes have already begun. Indeed, within days of Anthem's disclosure of the breach, Anthem warned that "phishing" schemes had been commenced. On its website Anthem now warns:

Members who may have been impacted by the cyber attack [], 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 click on any links in email.

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.

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

Anthem is not calling members regarding the cyber attack and is not asking for credit card information or social security numbers over the phone. 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.

44. For the rest of their lives, Plaintiffs and other members of the Class and Sub-

Classes will be forced to spend additional hours maintaining heightened diligence of all of their

accounts, medical policies, tax returns, etc., for fear of acts of identity theft against them and their families.

- 45. According the U.S. Department of Justice, victims of identity theft have had, among other things, bank accounts wiped out, credit histories ruined, and jobs and valuable possessions taken away. In some cases, they have even been arrested for crimes committed by others using their name. The financial toll exacted by identity theft can be crippling, and the emotional trauma can be as devastating. A Federal Reserve Bank of Boston document states that identity thieves often use a stolen identity again and again and that it is very common for victims to learn thieves have opened and accessed accounts spanning several years.
- 46. According to http://kaiserhealthnews.org/news/rise-of-indentity-theft/, the definition of medical identity theft is the fraudulent acquisition of someone's personal information name, Social Security number, health insurance number for the purpose of illegally obtaining medical services or devices, insurance reimbursements or prescription drugs. Pam Dixon, the founder and executive director of World Privacy Forum is quoted as stating "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," and "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."

COUNT I

NEGLIGENCE

- 47. Plaintiffs incorporate and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.
- 48. Anthem owed a duty of exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting personal and financial information in its possession from

being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Anthem's computer network securities systems to ensure that Plaintiffs and the other members of the Class and Sub-Classes' personal information in Anthem's possession were adequately secured and protected. Anthem further owed a duty to Plaintiffs and the other members of the Class and Sub-Classes to implement processes that would detect a breach of its security system and to prevent mass exports of highly sensitive information outside of the Anthem computer network.

- 49. Anthem owed a duty to Plaintiffs and the other members of the Class and Sub-Classes to provide security consistent with industry standards and requirements under the circumstances, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PII of Plaintiffs and the other members of the Class and Sub-Classes.
- 50. Anthem owed a duty of care to Plaintiffs and the other members of the Class and Sub-Classes because they were foreseeable and probable victims of a data breach given dated and inadequate computer systems and security practices. Anthem solicited, gathered, and stored the personal information for its own business purposes and in order to facilitate transactions with its Insureds. Anthem, in the absence of negligence, would have known that a breach of its systems would cause damages to Plaintiffs and the other members of the Class and Sub-Classes and that Anthem had a duty to adequately protect such sensitive PII.
- 51. Plaintiffs and the other members of the Class and Sub-Classes entrusted Anthem with their PII, based on their understanding that Anthem would safeguard their PII, and that Anthem was in a position to protect against the harm caused to Plaintiffs and the other members of the Class and Sub-Classes as a result of the data breach.

- 52. Anthem's own conduct created a foreseeable risk of harm to Plaintiffs and the other members of the Class and Sub-Classes. Anthem's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent and stop the data breach as set forth herein.
- 53. Anthem breached the duties it owed to Plaintiffs and the other members of the Class and Sub-Classes by failing to exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs and the other members of the Class and Sub-Classes.
- 54. Anthem breached the duties it owed to Plaintiffs and the other members of the Class and Sub-Classes by failing to properly implement technical systems or security practices that could have prevented the loss of the data at issue.
- 55. Anthem breached the duties it owed to Plaintiffs and the other members of the Class and Sub-Classes by failing to properly maintain their PII in Anthem's possession which has been stolen by hackers. Anthem, in the absence of negligence, should have known that Plaintiffs and the other members of the Class and Sub-Classes were foreseeable victims of a data breach of its systems because of applicable laws and statutes that require Anthem to reasonably safeguard sensitive PII. By its acts and omissions described herein, Anthem unlawfully breached this duty.
- 56. Plaintiffs and the other members of the Class and Sub-Classes were damaged by Anthem's breach of this duty.
- 57. The PII that was compromised by the breach of the Defendant's inadequate security included, without limitation, information that was being improperly stored and inadequately safeguarded by the Defendant. The breach of security was a direct and proximate result of the Defendant's failure to use reasonable care to implement and maintain appropriate

security procedures reasonably designed to protect the PII of Plaintiffs and the other members of the Class and Sub-Classes. This breach of security and unauthorized access to the private, nonpublic information of Plaintiffs and the other members of the Class and Sub-Classes was reasonably foreseeable, particularly in light of the April 2014 warnings regarding, among other things, the targeting by hackers of personal information maintained on the databases of health care companies.

- 58. The Defendant was in a special relationship of trust with Plaintiffs and the other members of the Class and Sub-Classes by reason of its entrustment with highly sensitive PII. By reason of this special relationship, Defendant had a duty of care to use reasonable means to keep the PII of the Class and Sub-Classes private and secure. The Defendant has unlawfully breached that duty.
- 59. Compromising and failing to maintain the privacy of Plaintiffs' and the other members of the Class and Sub-Classes' PII has directly and proximately caused an immediate harm and burden. Plaintiffs and the other members of the Class and Sub-Classes are now forced to be on a constant heightened lookout for signs of identity theft and will need to undertake numerous ongoing expenses and preventive (or remedial) measures because their PII is no longer private. Defendant knew or should have known that the network on which it stored the personal information of tens of millions of its Insureds had vulnerabilities and was at risk of breach by hackers. Defendant was negligent in continuing such data processing in light of those vulnerabilities and the sensitivity of the data.
- 60. As a direct and proximate result of the Defendant's conduct, Plaintiffs and the other members of the Class and Sub-Classes suffered damages including, but not limited to, loss of control of their PII, the burden and cost of heightened monitoring for signs for identity theft

and for undertaking actions such as credit freezes and alerts to prevent identity theft, and remediating acts and damages caused by identity theft, and other economic damages.

COUNT II

BREACH OF EXPRESS CONTRACT

- 61. Plaintiffs incorporate and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.
- 62. Anthem had an express contractual obligation to maintain the privacy and security of Plaintiffs' and the Class' PII.
- 63. Anthem stated to Plaintiffs and the Class, among other things, that the Company "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 . . . See https://www.anthem.com/ca/health-insurance/about-us/privacy#web.
- 64. Plaintiffs and the Class accepted Anthem's promise by purchasing, directly or indirectly, insurance and other services from Anthem and providing Anthem with their PII.
- 65. Anthem breached its promise to Plaintiffs and the Class by failing to maintain and sufficiently safeguard the Plaintiffs' and the Class' PII which was taken from Anthem by hackers.
- 66. The losses and damages suffered by the Plaintiffs and the Class alleged herein were the direct and proximate result of Anthem's breach of contract with the Plaintiffs and members of the Class.

COUNT III

BREACH OF IMPLIED CONTRACT

- 67. Plaintiffs incorporate and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.
- 68. By providing Plaintiffs' and the other Class and Sub-Classes members' PII to Anthem to purchase and maintain medical insurance policies and to arrange for payment and/or reimbursement for medical care under Anthem insurance policies, Plaintiffs and the other members of the Class and Sub-Classes entered into implied contracts with Anthem pursuant to which Anthem agreed to safeguard and protect such information from unauthorized access and theft.
- 69. Plaintiffs and the other members of the Class and Sub-Classes fully performed their obligations under the implied contracts with Anthem.
- 70. Defendant breached the implied contracts it had made with the Plaintiffs and the other members of the Class and Sub-Classes by failing to safeguard and protect the personal and financial information of Plaintiffs and the other members of the Class and Sub-Classes, and by allowing unauthorized access to the Anthem computer network and the mass exporting of PII from the Anthem.
- 71. The damages to Plaintiffs and the other members of the Class and Sub-Classes as described herein were the direct and proximate result of the Defendant's breaches of these implied contracts.

COUNT IV

UNJUST ENRICHMENT

- 72. Plaintiffs incorporate and re-allege all allegations contained in the preceding paragraphs as if fully set forth herein.
- 73. Plaintiffs and the other members of the Class and Sub-Classes conferred a monetary benefit upon Anthem in the form of premiums paid for the purchase of medical insurance policies from Anthem during the period of the data breach.
- 74. Anthem has knowledge of the benefits conferred directly upon it by Plaintiffs and the other members of the Class and Sub-Classes.
- 75. The monies paid for the purchase of insurance policies by Plaintiffs and the other members of the Class and Sub-Classes from Anthem during the period of data breach were supposed to be used by Anthem, in part, to pay administrative and other costs of providing reasonable data security and protection to Plaintiffs and the other members of the Class and Sub-Classes.
- 76. Anthem failed to provide reasonable security, safeguards and protection to the PII of Plaintiffs and the other members of the Class and Sub-Classes and, as a result, Plaintiffs and the other members of the Class and Sub-Classes overpaid Anthem for insurance services purchased during the period of the data breach.
- 77. Under principles of equity and good conscience, Anthem should not be permitted to retain the amounts paid for insurance service belonging to Plaintiffs and the other members of the Class and Sub-Classes, because Anthem failed to provide adequate safeguards and security measures to protect Plaintiffs' and the other members of the Class and Sub-Classes' PII that they paid for but did not receive.
- 78. As a result of Anthem's conduct as set forth in this Complaint, Plaintiffs and the other members of the Class and Sub-Classes suffered damages and losses as stated above, including monies paid for Anthem insurance policies that Plaintiffs and the other members of the

Class and Sub-Classes would not have purchased had Anthem disclosed the material fact that it lacked adequate measures to safeguard Insureds' PII data, and including the difference between the price paid for Anthem policies as promised and the actual diminished value of services received.

- 79. Plaintiffs and the other members of the Class and Sub-Classes have conferred directly upon Anthem an economic benefit in the nature of monies received and profits resulting from premiums paid and unlawful overcharges to the economic detriment of Plaintiffs and the other members of the Class and Sub-Classes.
- 80. The economic benefit, including premiums paid and the overcharges and profits derived by Anthem and paid by Plaintiffs and the other members of the Class and Sub-Classes, is a direct and proximate result of Anthem's unlawful practices as set forth in this Complaint.
- 81. The financial benefits derived by Anthem rightfully belong to Plaintiffs and the other members of the Class and Sub-Classes.
- 82. It would be inequitable under established unjust enrichment principles for Anthem to be permitted to retain any of the financial benefits, premiums, profits and overcharges derived from Anthem's unlawful conduct as set forth in this Complaint.
- 83. Anthem should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the other members of the Class and Sub-Classes all unlawful or inequitable premiums received by Anthem.
- 84. A constructive trust should be imposed upon all unlawful or inequitable sums received by Anthem traceable to Plaintiffs and the other members of the Class and Sub-Classes.

COUNT V

BAILMENT

- 85. Plaintiffs incorporate and re-allege all allegations contained in the preceding paragraphs as if fully set forth herein.
- 86. Plaintiffs and the other members of the Class and Sub-Classes delivered their PII to Anthem for the exclusive purpose of purchasing and utilizing insurance policies from Anthem.
- 87. In delivering their PII to Anthem, Plaintiffs and the other members of the Class and Sub-Classes intended and understood that Anthem would adequately safeguard their personal information.
- 88. Anthem accepted possession of Plaintiffs' and the other members of the Class and Sub-Classes' PII acting as an insurer of the Plaintiffs and the other members of the Class and Sub-Classes.
- 89. In accepting possession of Plaintiffs' and the other members of the Class and Sub-Classes' PII, Anthem understood that Plaintiffs and the other members of the Class and Sub-Classes expected Anthem to adequately safeguard their PII. Accordingly a bailment (or deposit) was established for the mutual benefit of the parties.
- 90. During the bailment (or deposit), Anthem owed a duty to Plaintiffs and the other members of the Class and Sub-Classes to exercise reasonable care, diligence and prudence in protecting their PII.
- 91. Anthem breached its duty of care by failing to take appropriate measures to safeguard Plaintiffs' and the other members of the Class and Sub-Classes' PII, resulting in the unlawful and unauthorized access and mass exporting of that information from Anthem's computer network to unauthorized recipients.
- 92. As a direct and proximate result of Anthem's breach of its duty, Plaintiffs and the other members of the Class and Sub-Classes suffered consequential damages that were reasonably foreseeable to Anthem, including but not limited to the damages sought herein.

- 93. As a direct and proximate result of Anthem's breach of its duty, the PII of Plaintiffs and the other members of the Class and Sub-Classes entrusted to Anthem during the bailment (or deposit) was forever damaged and its value diminished.
- 94. Plaintiffs and the other members of the Class and Sub-Classes have no adequate remedy at law.

COUNT VI

VIOLATIONS OF CALIFORNIA CONSUMER LAWS (ON BEHALF OF PLAINTIFF BLAIN AND THE CALIFORNIA SUB-CLASS)

- 95. Plaintiff Blain incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.
- 96. Plaintiff Blain and the other members of the California Sub-Class are consumers who purchased, directly or indirectly, insurance policies and services from Anthem for personal or family purposes.
- 97. Anthem engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Plaintiff and the other members of the California Sub-Class.
- 98. Anthem is engaged in, and its acts and omissions affect, trade and commerce.

 Anthem's acts, practices and omissions were done in the course of Anthem's business of marketing, offering for sale, and selling goods and services in the United States, including in the state of California.
- 99. Anthem's conduct, as alleged in this Complaint, including without limitation
 Anthem's failure to maintain adequate computer systems and data security practices to safeguard customers' PII, Anthem's failure to disclose the material fact that Anthem's computer systems and data security practices, was inadequate to safeguard Insureds' PII from theft.

100. Anthem's conduct constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices in violation of The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, et seq., and the California Unfair Competition Law, Cal. Bus. And Prof. Code, § 17200, et seq.

COUNT VII

VIOLATION OF THE CALIFORNIA DATA BREACH ACT (ON BEHALF OF PLAINTIFF BLAIN AND THE CALIFORNIA SUB-CLASS)

- 101. Plaintiff Blain incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.
- 102. The data breach described above constituted a "breach of the security system" of Anthem, within the meaning of Section 1798.82 (g) of the California Civil Code.
- 103. The information lost in the data breach constituted "personal information" within the meaning of Section 1798.80(e) of the California Civil Code.
- 104. Anthem failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.
- 105. Anthem unreasonably delayed informing anyone about the breach of security of Plaintiff and the California Sub-Class's confidential and non-public information after Anthem knew the data breach had occurred.
- 106. Anthem failed to disclose to Plaintiff Blain and the California Sub-Class, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII when they knew or reasonably believed such information had been compromised.
- 107. Upon information and belief, no law enforcement agency instructed Anthem that notification to Plaintiff Blain and the California Sub-Class would impede investigation.

- 108. As a result of Defendant's violation of Cal. Civ. Code § 1798.80 et seq., Plaintiff Blain and the California Sub-Class incurred economic damages, including expenses associated with necessary credit monitoring.
- 109. Plaintiff Blain, individually and on behalf of the California Sub-Class, seeks all remedies available under Cal. Civ. Code § 1798.84, including but not limited to: (a) damages suffered by the California Sub-Class as alleged above; (b) statutory damages for Anthem's willful, intentional, and/or reckless violation of Cal. Civ. Code § 1798.83; and (c) equitable relief.
- 110. Plaintiff Blain, individually and on behalf of the California Sub-Class, also seeks reasonable attorneys' fees and costs under Cal. Civ. Code § 1798.84(g).

COUNT VIII

VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT (ON BEHALF OF PLAINTIFF BLAIN AND THE CALIFORNIA SUB-CLASS)

- 111. Plaintiff Blain incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.
- 112. Anthem is a provider of health care within the meaning of Civil Code § 56.06(a) and maintains medical information as defined by Civil Code § 56.05(g).
- 113. Plaintiff Blain is a patient of Anthem as defined in Civil Code § 56.05(h).

 Anthem maintains personal medical information of Plaintiff Blain and the other members of the California Sub-Class.
- 114. Anthem misused and/or disclosed medical information regarding Plaintiff Blain and other members of the California Sub-Class without written authorization compliant with the provisions of Civil Code § 56, et seq.

- 115. Anthem's misuse and/or disclosure of medical information regarding the Plaintiff Blain and the California Sub–Class constitute a violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.
- 116. Plaintiff Blain and the California Sub-Class suffered damages from the improper misuse and/or disclosure of their medical information. Therefore, Plaintiff Blain and the California Sub-Class seek relief under Civil Code §§ 56.35 and 56.36.
- 117. Plaintiff Blain and the California Sub-Class seek actual damages, statutory damage, statutory penalties, attorney fees and costs pursuant to Civil Code §§ 56.35 and 56.36.

COUNT IX

VIOLATIONS OF NEW YORK'S CONSUMER PROTECTION LAWS (ON BEHALF OF PLAINTIFF KALFA AND THE NEW YORK SUB-CLASS)

- 118. Plaintiff Kalfa incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.
- 119. Anthem's practices, acts, policies and course of conduct, as described above, including making representations that it possessed sufficient security to maintain the privacy of such PII, were intended to induce, and did induce, Plaintiff Kalfa and the New York Sub-Class to provide their sensitive PII to Anthem.
- 120. Plaintiff Kalfa and the New York Sub-Class never would have provided their sensitive and personal PII if they had been told or knew that Anthem failed to maintain sufficient security to keep such PII from being hacked and taken by others, and that Anthem failed to maintain the information in encrypted form.
 - 121. Anthem's practices, acts, policies and course of conduct are actionable in that:

- (a) Anthem actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff Kalfa and the New York Sub-Class at the time they provided such PII information that Anthem had sufficient security or mechanisms to protect PII; and
- (b) Anthem failed to give adequate warnings and notices regarding the defects and problems with its defective system orsecurity systems that it maintained to protect Plaintiff Kalfa and the New York Sub-Class' PII. Anthem possessed prior knowledge of the inherent defects in Anthem's system of security and failed to give adequate and timely warnings that there had been a data breach and hacking episodes had occurred.
- 122. The aforementioned conduct is and was deceptive, false, fraudulent and constitutes an unconscionable commercial practice in that Anthem has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system it maintained and failed to reveal the data breach timely and adequately.
- 123. Members of the public were deceived by and relied upon Anthem's affirmative misrepresentations and failures to disclose.
- 124. Such acts by Anthem are and were deceptive acts or practices which are and/or were, likely to mislead a reasonable consumer providing their PII to Anthem. Said deceptive acts and practices aforementioned are material. The requests for and use of such PII materials in New York and concerning New York residents and/or citizens was a consumer-oriented act and thereby falls under the New York consumer fraud statute, General Business Law § 349 and § 350.
- 125. Anthem's wrongful conduct caused Plaintiff Kalfa and the New York Sub-Class to suffer a consumer-related injury by causing them to incur substantial expense to protect from

misuse of the PII materials by third parties and placing Plaintiff Kalfa and the New York Sub-Class at serious risk for monetary damages.

126. In addition to or in lieu of actual damages, because of the injury, Plaintiff Kalfa and the Sub-Class seek statutory damages for each injury and violation which has occurred.

COUNT X

VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT (ON BEHALF OF PLAINTIFF BERNSTEIN AND THE NEW JERSEY SUB-CLASS)

- 127. Plaintiff Bernstein incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein. This claim is brought pursuant to New Jersey statute 56:8-2, et seq. ("The New Jersey Consumer Fraud Act").
- 128. The New Jersey Consumer Fraud Act prohibits the "use or employment by any person of any unconscionable commercial practice, deception or fraud, false pretense, false promise or misrepresentation, or the knowing concealment, suppression or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate...is declared to be an unlawful practice..."
- 129. Plaintiff Bernstein and the New Jersey Sub-Class never would have provided their sensitive and personal PII if they had been told or knew that Anthem failed to maintain sufficient security to keep such PII from being hacked and taken by others, that Anthem failed to maintain the information in encrypted form.
 - 130. Anthem's practices, acts, policies and course of conduct are actionable in that:
- (a) Anthem actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff Bernstein and the New Jersey Sub-Class at the time they provided their PII information that Anthem did not have sufficient security or mechanisms to protect PII; and

- (b) Anthem failed to give adequate warnings and notices regarding the defects and problems with its defective system of security that it maintained to protect Plaintiff Bernstein and the New Jersey Sub-Class' PII. Anthem possessed prior knowledge of the inherent defects in Anthem's system of security and failed to give adequate and timely warnings that there had been a data breach and hacking episodes had occurred.
- 131. The aforementioned conduct is and was deceptive, false, fraudulent and constitutes an unconscionable commercial practice in that Anthem has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system it maintained and failed to reveal the data breach timely and adequately.
- 132. Members of the New Jersey Sub-Class were deceived by and relied upon Anthem's affirmative misrepresentations and failures to disclose.
- 133. Such acts by Anthem are and were deceptive acts or practices which are and/or were, likely to mislead a reasonable consumer providing their PII to Anthem. Said deceptive acts and practices aforementioned are material. The requests for and use of such PII materials in New Jersey and concerning New Jersey residents and/or citizens was a consumer-oriented and thereby falls under the New Jersey Consumer Fraud Act.
- 134. Anthem's wrongful conduct caused Plaintiff Bernstein and the New Jersey Sub-Class to suffer a consumer-related injury and ascertainable losses by causing them to incur substantial expense to protect from misuse of the PII materials by third parties and placing Plaintiff Bernstein and the Sub-Class at serious risk for monetary damages.
- 135. In addition to or in lieu of actual damages, because of the injury, Plaintiff
 Bernstein and the New Jersey Sub-Class seek treble damages, attorneys' fees and costs for each injury and violation which has occurred.

COUNT XI

VIOLATIONS OF THE NEW HAMPSHIRE CONSUMER FRAUD ACT (ON BEHALF OF PLAINTIFF MULDOON AND THE NEW HAMPSHIRE SUB-CLASS)

- 136. Plaintiff Muldoon incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein. This claim is brought pursuant to N.H. RSA § 358-A:2, et. seq. (the "New Hampshire Consumer Fraud Act").
- 137. The New Hampshire Consumer Fraud Act prohibits any person from using any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce within the state of New Hampshire.
- 138. Plaintiff Muldoon and the New Hampshire Sub-Class never would have provided their sensitive and personal PII if they had been told or knew that Anthem failed to maintain sufficient security to keep such PII from being hacked and taken by others or that Anthem failed to maintain the information in encrypted form.
 - 139. Anthem's practices, acts, policies and course of conduct are actionable in that:
- (a) Anthem actively and knowingly misrepresented to Plaintiff Muldoon and the New Hampshire Sub-Class at the time of providing such information that Anthem had sufficient security or mechanisms to protect PII; and
- (b) Anthem failed to give adequate warnings and notices regarding the defects and problems with its defective system of security that it maintained to protect Plaintiff Muldoon and the New Hampshire Sub-Class' PII. Anthem possessed prior knowledge of the inherent defects in Anthem's system of security and failed to give adequate and timely warnings that there had been a data breach and hacking episodes had occurred.
- 140. The aforementioned conduct is and was deceptive, false, fraudulent and constitutes an unconscionable commercial practice in that Defendant has, by the use of false or

deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system it maintained and failed to reveal the data breach timely and adequately.

- 141. Members of the New Hampshire Sub-Class were deceived by and relied upon Anthem's affirmative misrepresentations and failures to disclose.
- 142. Such acts, omissions and misrepresentations by Anthem are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing their PII to Anthem. Said deceptive acts and practices aforementioned are material. The requests for and use of such PII materials in New Hampshire and concerning New Hampshire residents and/or citizens was consumer-oriented and thereby falls under the New Hampshire Consumer Fraud Act.
- 143. Anthem's wrongful conduct caused Plaintiff Muldoon and the New Hampshire Sub-Class to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of the PII materials by third parties and placing Plaintiff Muldoon and the New Hampshire Sub-Class at serious risk for monetary damages.
- 144. In addition to or in lieu of actual damages, because of the injury, Plaintiff
 Muldoon and the New Hampshire Sub-Class seek damages, equitable relief, attorneys' fees and
 costs for each injury and violation which has occurred.

COUNT XII

VIOLATION OF THE NEW HAMPSHIRE DATA BREACH ACT (ON BEHALF OF PLAINTFF MULDOON AND THE NEW HAMPSHIRE SUB-CLASS)

145. Plaintiff Muldoon incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.

- 146. The data breach described above constituted a "security breach" of Anthem, within the meaning of N.H. RSA §§ 359-C:19, C:20 and C:21.
- 147. The information lost in the data breach constituted "personal information" within the meaning of N.H. RSA §§ 359-C:19, C:20 and C:21.
- 148. Anthem failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.
- 149. Anthem unreasonably delayed informing anyone about the breach of security of Plaintiff Muldoon and the New Hampshire Sub-Class' confidential and non-public information after Anthem knew the data breach had occurred.
- 150. Anthem failed to notify Plaintiff Muldoon and the New Hampshire Sub-Class, as soon as possible, after it determined that misuse of PII had occurred or is reasonably likely to occur as required pursuant to N.H. RSA §§ 359-C:19, C:20 and C:21.
- 151. Upon information and belief, no law enforcement agency, or national or homeland security agency instructed Anthem that notification to Plaintiff Muldoon and the New Hampshire Sub-Class would impede investigation.
- 152. As a result of Anthem's violations of N.H. RSA §§ 359-C:19, C:21, C:21, Plaintiff Muldoon and the New Hampshire Sub-Class incurred economic damages, including expenses associated with necessary credit monitoring.
- 153. Plaintiff Muldoon, individually and on behalf of the New Hampshire Sub-Class, seeks all remedies available under N.H. RSA §§ 359-C:19, C:21 and C:21, including but not limited to: (a) damages suffered by the New Hampshire Sub-Class as alleged above; (b) statutory damages for Anthem's willful or knowing violation of New Hampshire Revised Statute §§ 359-C:19, C:21 and C:21; and (c) equitable relief. Plaintiff Muldoon, individually and on behalf of

the New Hampshire Sub-Class, also seeks reasonable attorneys' fees and costs under N.H. RSA §§ 359-C:19, C:21 and C:21.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully request the following relief:

- a. that this Court certify this action as a Class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), and appoint the Plaintiffs as Class and Sub-class representatives and their counsel as Class counsel;
- b. that this Court enter judgment in favor of Plaintiffs and the other members of the Class and Sub-Classes, and against the Defendant under the legal theories alleged herein;
- c. that this Court award Plaintiffs and the other members of the Class and Sub-Classes appropriate relief, including actual and statutory damages, restitution and disgorgement;
 - d. that this Court award attorney's fees, expenses, and costs of this suit;
- e. that this Court award the Plaintiffs and the other members of the Class and Sub-Classes pre-judgment and post-judgment interest at the maximum rate allowable by law;
- f. that the Court award the Plaintiffs and the other members of the Class and Sub-Classes equitable, injunctive and declaratory relief as may be appropriate under applicable laws. Plaintiffs on behalf of the other members of the Class and Sub-Classes seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing reasonable data security practices to safeguard customers' financial and personal information, by an Order requiring Anthem to implement reasonable data security enhancements as they become available, including data encryption, segregation of sensitive data,

more robust passwords, authentication of users, increased control of access to sensitive information on the network, prohibitions of mass exports of sensitive data;

g. that this Court enter such additional orders or judgment as may be necessary to prevent the Customer Data Breach from recurring and to restore any interest or any money or property which may have been acquired by means of violations set forth in this Complaint;

h. that this Court award such other and further relief as it may deem just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs, individually and on behalf of all others similarly situated, demand a trial by jury on all issues so triable.

DATED: February 20, 2015

COHEN & MALAD, LLP

Irwin B. Levin Richard E. Shevitz Scott D. Gilchrist

Scott D. Gilchilst

Vess A. Miller

One Indiana Square, Suite 1400

Indianapolis, IN 46204 Phone: (317) 636-6481

Fax: (317) 636-2593

more robust passwords, authentication of users, increased control of access to sensitive information on the network, prohibitions of mass exports of sensitive data;

- g. that this Court enter such additional orders or judgment as may be necessary to prevent the Customer Data Breach from recurring and to restore any interest or any money or property which may have been acquired by means of violations set forth in this Complaint;
- h. that this Court award such other and further relief as it may deem just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs, individually and on behalf of all others similarly situated, demand a trial by jury on all issues so triable.

DATED: February 20, 2015

COHEN & MALAD, LLP

Irwin B. Levin, #8786-49

Richard E. Shevitz, #12007-49

Scott D. Gilchrist, #16720-53

Vess A. Miller, #26495-53

Lynn A. Toops, #26386-49

One Indiana Square, Suite 1400

Indianapolis, IN 46204

Phone: (317) 636-6481 Fax: (317) 636-2593

STULL, STULL & BRODY

Howard Longman, Esq. Patrick Slyne, Esq. Melissa Emert, Esq. 6 East 45th Street New York, NY 10017 (212) 687-7230 (telephone) (212) 490-2022 (facsimile)

KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.

Gary S. Graifman, Esq. Robert Lubitz, Esq. 747 Chestnut Ridge Road Chestnut Ridge, New York 10977 Tel: (845) 356-2570 (telephone) Fax: (845) 356-4335 (facsimile)

Counsel for Plaintiffs