Daniel C. Girard (SBN 114826)
Eric H. Gibbs (SBN 178658)
Scott M. Grzenczyk (SBN 279309)
Steven A. Lopez (SBN 300540)
GIRARD GIBBS LLP
601 California Street, 14th Floor
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
Email: dcg@girardgibbs.com

Attorneys for Plaintiff Aswad Hood

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

ASWAD HOOD, on behalf of himself and all others similarly situated,

Plaintiff,

vs.

ANTHEM, INC., BLUE CROSS OF CALIFORNIA, and ANTHEM BLUE CROSS LIFE AND HEALTH INSURANCE COMPANY,

Defendants.

Case No.

CLASS ACTION

COMPLAINT FOR RELIEF BASED ON:

(1) Violation of the California Customer Records Act;
(2) Violation of the California Unfair Competition Law;
(3) Breach of Contract; and
(4) Negligence

DEMAND FOR JURY TRIAL

SUMMARY OF THE CASE

1. On February 4, 2015, Anthem, Inc. announced that hackers had breached the company's database warehouse and obtained the personal information of approximately 80 million current and former Anthem health insurance plan members and Anthem employees. The personal information obtained in the breach included plan members' and employees' names, birthdays, medicals IDs, Social Security numbers, addresses, email addresses, and employment information, including income.

2. Plan members' and employees' personal information has been exposed – and their identities put at risk – because Anthem failed to maintain reasonable and adequate security measures. Anthem has statutory obligations to protect the sensitive personal information it maintains, yet failed at numerous opportunities to prevent, detect, or limit the scope the breach. Among other things, Anthem (1) failed to implement security measures designed to prevent this attack even though the health care industry has been repeatedly warned about the risk of cyber-attacks, (2) failed to employ security protocols to detect the unauthorized network activity, and (3) failed to maintain basic security measures such as complex data encryption so that if data were accessed or stolen it would be unreadable.

3. Plaintiff is a current Anthem Blue Cross plan member who brings this proposed class action lawsuit on behalf of Anthem health plan members and Anthem employees whose personal information has been compromised as a result of the data breach. He seeks injunctive relief requiring Anthem to implement and maintain security practices to comply with regulations designed to prevent and remedy these types of breaches, as well as restitution, damages, and other relief.

PARTIES

4. Plaintiff Aswad Hood is a resident of Los Angeles, California.

5. Defendant Anthem, Inc. is an Indiana corporation with its principal place of business in Indianapolis, Indiana. Anthem, Inc. was formerly known as WellPoint, Inc. and changed its name on December 3, 2014.

6. Defendant Blue Cross of California is a California corporation with its principal place of business in Indianapolis, Indiana. Blue Cross of California operates under the trade name Anthem Blue Cross.

7. Defendant Anthem Blue Cross Life and Health Insurance Company is a California corporation with its principal place of business in Indianapolis, Indiana.

8. Defendants Anthem, Inc., Blue Cross of California, and Anthem Blue Cross Life and Health Insurance Company are collectively referred to as Anthem.

JURISDICTION AND VENUE

9. This Court has original jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because (a) at least one member of the putative class is a citizen of a state different from Anthem, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, (c) the proposed class consists of more than 100 class members, and (d) none of the exceptions under the subsection apply to this action.

10. This Court has jurisdiction over Defendants because they are registered to conduct business in California, have sufficient minimum contacts in California, or otherwise intentionally avail themselves of the markets within California, through the promotion, sale, marketing and distribution of their products in California, to render the exercise of jurisdiction by this Court proper and necessary. Defendants Blue Cross of California and Anthem Blue Cross Life and Health Insurance Company are incorporated in California.

11. Venue is proper in this District under 28 U.S.C. § 1391 because Plaintiff resides in this district, Defendants conduct substantial business in this District, and a substantial part of the events giving rise to Plaintiff's claims occurred in this District.

COMMON FACTUAL ALLEGATIONS

The Data Breach

12. Anthem is one of the country's largest health plan providers. On February 4, 2015, the company announced that hackers had breached its network and obtained the

personal information of approximately 80 million Anthem health insurance plan members and Anthem employees. The affected brands and plans are Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, Caremore, and Unicare as well as members of the Blue Cross and Blue Shield Association's BlueCard program. The information obtained by the hackers includes names, birthdays, medicals IDs, Social Security numbers, addresses, email addresses, and employment information, including income.

13. The hackers accessed Anthem's database by using login credentials of five Anthem technicians. According to Anthem, an unauthorized attempt to access its system occurred on December 10, 2014, and may have occurred earlier in 2014.[1]

14. The hackers successfully penetrated Anthem's system sometime after December 10, 2014. According to Anthem, the company did not detect the unauthorized network activity until January 27, 2015, when an Anthem computer administrator discovered that other individuals had been using his login credentials to access Anthem's network and obtain data. Reports indicate, however, that Anthem's website dedicated to the security breach – www.anthemfacts.com – was registered on December 13, 2014.[2]

15. Anthem has not notified affected plan members and employees of the data breach. Instead, Anthem has said that it will begin mailing letters to individuals whose personal information was compromised "in the coming weeks."[3] As a result, many class members will be unaware that their personal information has been compromised and therefore will not timely take the steps necessary to safeguard themselves from the improper use of that information.

---

[1] Brandon Bailey, *Anthem Hackers Tried to Breach System as Early as December*, HUFFINGTON POST, http://www.huffingtonpost.com/2015/02/06/anthem-hackers-december_n_6634440.html (last visited Feb. 8, 2015).

[2] Dan Goodin, *String of big data breaches continues with hack on health insurer Anthem*, ARSTECHNICA, http://arstechnica.com/security/2015/02/string-of-big-data-breaches-continues-with-hack-on-health-insurer-anthem/ (last visited Feb. 8, 2015).

[3] Anthem Data Breach FAQ, http://www.anthemfacts.com/faq (last visited Feb. 8, 2015).

Anthem's Security Practices are Inadequate

16. Health care providers are frequently the target cyber-attacks because their networks store large amounts of sensitive personal information. Health care data is far more valuable on the black market than credit card or other personal information, and businesses that store such information are therefore likely to be targeted by cybercriminals. Unlike credit card and bank account numbers, information maintained by health care companies – such as date of birth and Social Security number – are not easily destroyed and can be used to perpetrate identify theft and other types of frauds. Medical information is highly valuable and is reportedly "worth 10 times more than [a person's] credit card number on the black market."[4] According to a security expert, at a black market auction credit card records were selling for $0.33 while one patient's medical records sold for $251.[5]

17. According to industry experts, "cyber criminals are increasingly targeting the $3 trillion U.S. healthcare industry, which has many companies still reliant on aging computer systems that do not use the latest security features."[6] Daniel Nutkis, the chief executive of the Health Information Trust Alliance, a healthcare industry group that works with companies to improve data security, stated that "the industry has become, over the last three years, a much bigger target."[7] A report prepared by the Ponemon

[4] Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit card*, REUTERS, http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924 (last visited Feb. 8, 2015).

[5] Reed Abelson and Julie Creswell, *Data Brach at Anthem May Lead to Others*, NY TIMES, http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html (last visited Feb. 8, 2015).

[6] Supriya Kurane and Jim Finkle, *Health insurer Anthem hit by massive cybersecurity breach*, REUTERS, http://www.reuters.com/article/2015/02/06/us-anthem-cybersecurity-idUSKBN0L907J20150206 (last visited Feb. 8, 2015).

[7] *Abelson*, *supra* note 5.

Institute estimated that 90% of health care organizations have incurred at least one data breach over the last two years.[8]

18. On April 8, 2014, the Federal Bureau of Investigation issued a Private Industry Notification to healthcare providers, warning them that their cybersecurity systems are inadequate.[9] According to the notification, "[t]he 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." Particularly in light of recent data breaches at numerous large retailers – including Target, Home Depot, and JPMorgan Chase – Anthem knew or should have known that its computers systems were vulnerable.

19. The FBI notification also cites a report prepared by the SANS Institute that warned that the healthcare industry was not sufficiently prepared to combat cyber-attacks. The SANS Health Care Cyber Threat Report analyzed data collected between September 2012 and 2013 and found the results to be "alarming."[10] The report explained that "[t]he data not only confirmed how vulnerable the industry had become, it also revealed how far behind industry-related cybersecurity strategies and controls have fallen."

20. In August 2014 – after a cyber-attack on Community Health Systems, Inc. – the FBI warned companies within the healthcare industry that hackers were targeting them.[11] The warning stated that "[t]he FBI has observed malicious actors targeting

---

[8] *Id.*

[9] Jim Finkle, *Exclusive: FBI wants healthcare sector vulnerable to cyberattacks*, REUTERS, http://www.reuters.com/article/2014/04/23/us-cybersecurity-healthcare-fbi-exclusiv-idUSBREA3M1Q920140423 (last visited Feb. 8, 2015).

[10] SANS INSTITUTE, HEALTH CARE CYBERTHREAT REPORT: WIDESPREAD COMPROMISES DETECTED, COMPLIANCE NIGHTMARE ON HORIZON 2 (2014), *available at* http://pages.norse-corp.com/rs/norse/images/Norse-SANS-Healthcare-Cyberthreat-Report2014.pdf (last visited Feb. 8, 2015).

[11] Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, REUTERS, http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited Feb. 8, 2015).

healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."

21. One of the key methods companies can use to protect sensitive information – including their customers' personal information – is through a process known as encryption. Encryption is the process of altering information in a way that only someone with a 'key' is able to change the data back to its original, readable form. Encryption is the second stage of data protection. The first is limiting access to the data itself. In the event that data is stolen or otherwise accessed by an unauthorized user, complex encryption prevents the data from being read and understood unless the unauthorized users also obtain the key. Encryption is the last, and a critical, defense against hackers and data breaches.

22. The United States Department of Health and Human Services' Office for Civil Rights urges health care providers and insurers to encrypt data containing sensitive personal information. In April 2014 the Department fined Concentra Health Services and QCA Health Plan Inc. of Arkansas approximately two million dollars for failing to encrypt laptops containing customer information.[12] In announcing the fines, Susan McAndrew, the DHHS' Office of Human Rights' deputy director of health information privacy, stated "[our] message to these organizations is simple: encryption is your best defense against these incidents."

23. Despite growing efforts by hackers to access personal information maintained by health care companies and the emphasis on data security in the health care field, Anthem (1) failed to implement security measures designed to prevent this attack even though the health care industry has been repeatedly warned about the risk of cyber-attacks, (2) failed to employ security protocols to detect the unauthorized network activity, and (3) failed to maintain basic security measures such as complex data

[12] U.S. Department of Health and Human Services, Stolen Laptops Lead to Important HIPAA Settlements (Apr. 22, 2104), *available at* http://www.hhs.gov/news/press/2014pres/04/20140422b.html (last visited Feb. 8, 2015).

encryption so that if data were accessed or stolen it would be unreadable. According to an Anthem spokesperson, while the company encrypts data when it moves in and out of data warehouses, it does not encrypt the information while it is stored in database warehouses.[13] The lack of encryption will make it much easier for hackers to read and understand the data they obtained.

Current and Former Anthem Health Plan Members and Anthem Employees Are Victims of the Breach

24. As a result of Anthem's negligent security practices and the delay in notifying affected customers, former and current Anthem health plan members and employees are subject to an increased and concrete risk of identity theft based on the Anthem's exposure of their personal information. James P. Nehf, professor at the Indiana University Robert H. McKinney School of Law, described the information obtained in the Anthem data breach as gold for criminals.[14] According to Professor Nehf, the information is more valuable than credit card or bank account information because it allows criminals to impersonate victims in a variety of harmful and damaging ways.

25. Former and current Anthem plan members and employees will have to spend time and money securing their personal information and protecting their identities. They will need to monitor their accounts and credit, and will also have to pay for credit monitoring or credit reports in the wake of the data breach to make sure that their credit and identity is not harmed by anyone who may have stolen their information. Individuals whose bank accounts are compromised may have to pay fees to their banks for new debit and credit cards, or have to pay fees to have the cards shipped faster so that they do not have to wait weeks to make purchases on their accounts.

---

[13] Bill Berkrot, *Anthem warns U.S. customers of email scam after data breach*, REUTERS, http://www.reuters.com/article/2015/02/06/us-anthem-cybersecurity-warning-idUSKBN0LA24F20150206 (last visited Feb. 8, 2015).

[14] Tim Evans, *Anthem data breach: How to protect yourself*, USA TODAY, http://www.usatoday.com/story/tech/2015/02/05/anthem-data-breach-protect-customers/22934777/ (last visited Feb. 8, 2015).

26. The disclosure of Social Security numbers in particular poses significant risks. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Former and current Anthem plan members and employees whose Social Security numbers have been compromised have spent time contacting various agencies, such as the Internal Revenue Service, the Social Security Administration, and their local state tax boards. They also now face a real and immediate risk of identity theft and other problems associated with the disclosure of their Social Security number, and will need to monitor their credit and tax filings for an indefinite duration. Individuals cannot even obtain a new Social Security number *until* there is evidence of ongoing problems due to misuse of the Social Security number. Even then, the Social Security Administration warns "that a new number probably will not solve all [] problems . . . and will not guarantee [] a fresh start." "For some victims of identity theft, a new number actually creates new problems."[15]

27. Anthem has provided little-to-no information about how affected customers can protect themselves. The company has not provided concrete information about when it will notify individuals whose data was compromised, instead saying it will mail notice of the data breach "in the coming weeks." The FAQ on its website states that the notice will "advise [impacted members] of the protections being offered to them as well as any next steps."[16] It provides no other information or guidance about what steps class members can take to protect their identities and minimize the damage arising from the data breach.

28. Other hackers have already taken advantage of the Anthem data breach in an attempt to obtain class members' personal information. Class members have received emails falsely claiming to be from Anthem and asking recipients to click on a link to

[15] *Identity Theft And Your Social Security Number*, Social Security Administration (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Feb. 8, 2015).

[16] Anthem Data Breach FAQ, *supra* note 3.

obtain credit monitoring or provide their social security number.[17] Fraudulent emails entitled "Your Turbotax account: update your information" have also sought to capitalize on the Anthem data breach by tricking potentially affected individuals into handing over their personal information under the false pretense of updating their Turbotax records.

29. One example of the impact data breaches have had is the rise in fraudulent tax filings. Kentucky delayed the issuance of tax refunds in response to concerns over fraudulent claims.[18] On February 5, 2015, Intuit – which operates Turbotax – temporarily stopped processing tax returns for 24 hours because of a rise in fraudulent state tax filings.[19] The state of Connecticut delayed the payment of tax refunds in the wake of the Anthem data breach.[20]

30. Experts have also suggested that the breach of Anthem's network may lead hackers to increasingly target other healthcare companies.[21]

PLAINTIFF HOOD'S EXPERIENCE

31. Plaintiff Aswad Hood is a resident of Los Angeles, California. Mr. Hood works for Los Angeles County and has health insurance coverage through Anthem for himself and his family. Mr. Hood and his family became members of an Anthem Blue Cross health insurance plan in October 2014. Anthem obtained their sensitive personal

---

[17] Berkrot, *supra* note 13.

[18] Michaela MacDonald, *Kentucky temporarily delays electronic tax returns*, WHAS 11 ABC, http://www.whas11.com/story/news/2015/02/06/kentucky-temporarily-delays-electronic-tax-returns/23019767/ (last visited Feb. 8, 2015).

[19] INTUIT WORKING WITH STATE GOVERNMENTS TO SOLVE EMERGING TAX FRAUD PROBLEM, http://investors.intuit.com/press-releases/press-release-details/2015/Intuit-Working-With-State-Governments-to-Solve-Emerging-Tax-Fraud-Problem/default.aspx (last visited Feb. 8, 2015).

[20] *ID Concerns Prompt DRS t0 Delay Mailing Refunds, Suggest Filing Early*, CBS CONNECTICUT, http://connecticut.cbslocal.com/2015/02/06/id-concerns-prompt-drs-to-delay-mailing-refunds-suggest-filing-early/ (last visited Feb. 8, 2015).

[21] *Abelson*, *supra* note 5.

information, including their birthdays, social security numbers, address, email addresses, and employment information.

32. Plaintiff Hood learned of the Anthem data breach from watching the news on television. He has not received notice of the breach from Anthem. The Anthem data breach has compromised the personal data of Mr. Hood, his wife, and three children, including their birthdays, medical IDs, social security numbers, address, and email addresses. Due to Anthem's conduct, Plaintiff Hood's family is now at a heightened risk for future identity theft

CLASS ACTION ALLEGATIONS

33. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and the classes preliminarily defined as:

California Class

> Current and former members of an Anthem health insurance plan and Anthem employees in California whose personal information was compromised as a result of the data breach announced in February 2015.

Nationwide Class

> Current and former members of an Anthem health insurance plan and Anthem employees in the United States whose personal information was compromised as a result of the data breach announced in February 2015.

Excluded from the proposed classes are anyone employed by counsel for Plaintiff in this action and any Judge to whom this case is assigned, as well as his or her staff and immediate family.

34. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy prerequisites for suing as a representative party pursuant to Rule 23.

35. Numerosity. The proposed classes consist of tens of millions of former or current Anthem health insurance plan members and employees who had their data stolen in the Anthem data breach, making joinder of each individual class member impracticable.

36. Commonality. Common questions of law and fact exist for the proposed classes' claims and predominate over questions affecting only individual class members. Common questions include:

a. Whether Anthem violated California Civil Code sections 1798.81.5 by failing to implement reasonable security procedures and practices;

b. Whether Anthem violated California Civil Code section 1798.82 by failing to promptly notify class members that their personal information had been compromised;

c. Whether Anthem acted negligently in failing to maintain adequate security procedures and practices;

d. Whether Anthem breached its contractual promises to adequately protect class members' personal information;

e. Whether Anthem's failure to implement adequate security constitutes an unfair, unlawful, or deceptive practice under state consumer protection law;

f. Whether class members may obtain damages, restitution, declaratory, and injunctive relief against Anthem; and

g. What security procedures and data-breach notification procedure Anthem should be required to implement as part of any injunctive relief ordered by the Court.

37. Typicality. Plaintiff's claims are typical of the claims of the proposed classes because, among other things, Plaintiff and class members sustained similar injuries as a result of Anthem's uniform wrongful conduct and their legal claims all arise from the same core Anthem practices.

38. Adequacy. Plaintiff will fairly and adequately protect the interests of the classes. His interests do not conflict with class members' interests and he has retained counsel experienced in complex class action and data privacy litigation to vigorously prosecute this action on behalf of the classes.

39. In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual class members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing Anthem's conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

40. In addition, class certification is appropriate under Rule 23(b)(1) or (b)(2) because:

a. the prosecution of separate actions by the individual members of the proposed classes would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Anthem;

b. the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and

c. Anthem has acted or refused to act on grounds that apply generally to the proposed classes, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed classes as a whole.

FIRST CAUSE OF ACTION

For Violation of the California Customer Records Act,

California Civil Code Section 1798.80, *et seq.*

41. Plaintiff incorporates the above allegations by reference.

42. Plaintiff brings this cause of action on behalf of the California Class whose personal information is maintained by Anthem and/or that was compromised in the data breach announced in February 2015.

43. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted California Customer Records Act. This statute states that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Civil Code section 1798.81.5.

44. Anthem is a "business" within the meaning of Civil Code section 1798.80(a).

45. Plaintiff and members of the class are "individual[s]" within the meaning of the Civil Code section 1798.80(d). Pursuant to Civil Code sections 1798.80(e) and 1798.81.5(d)(1)(C), "personal information" includes an individual's name, Social Security number, driver's license or state identification card number, debit card and credit card information, medical information, or health insurance information. "Personal information" under Civil Code section 1798.80(e) also includes address, telephone number, passport number, education, employment, employment history, or health insurance information.

46. The breach of the personal data of tens of millions of former or current Anthem health insurance plan members and Anthem employees constituted a "breach of the security system" of Anthem pursuant to Civil Code section 1798.82(g).

47. By failing to implement reasonable measures to protect its former and current health insurance plan members' and its employees' personal data, Anthem violated Civil Code section 1798.81.5.

48. In addition, by failing to promptly notify all affected former and current Anthem plan members and employees that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach, Anthem violated Civil Code section 1798.82 of the same title. Anthem's failure to timely notify employees of the breach has caused damage to class members who have had to buy identity protection services or take other measures to remediate the breach caused by Anthem's negligence.

49. By violating Civil Code sections 1798.81.5 and 1798.82, Anthem "may be enjoined" under Civil Code section 1798.84(e).

50. Accordingly, Plaintiff requests that the Court enter an injunction requiring Anthem to implement and maintain reasonable security procedures to protect customers' data in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that Anthem, 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 Anthem's systems on a periodic basis; (2) ordering that Anthem engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Anthem audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Anthem, consistent with industry standard practices, conduct regular database scanning and securing checks; (5) ordering that Anthem, 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; (6) ordering Anthem to meaningfully educate its former and current members and employees about the threats they face as a result of the loss of their personal information to third parties, as well as the

steps they must take to protect themselves; and (7) ordering Anthem to encrypt sensitive personal information.

51. Plaintiff further requests that the Court require Anthem to (1) identify and notify all members of the class who have not yet been informed of the data breach; and (2) to notify affected former and current members and employees of any future data breaches by email within 24 hours of Anthem's discovery of a breach or possible breach and by mail within 72 hours.

52. As a result of Anthem's violation of Civil Code sections 1798.81.5, and 1798.82, Plaintiff and members of the class have and will incur economic damages relating to time and money spent remedying the breach, including but not limited to, expenses for bank fees associated with the breach, any unauthorized charges made on financial accounts, lack of access to funds while banks issue new cards, tax fraud, as well as the costs of credit monitoring and purchasing credit reports.

53. Plaintiff, individually and on behalf of the members of the California Class, seeks all remedies available under Civil Code section 1798.84, including, but not limited to: (a) damages suffered by members of the class; and (b) equitable relief.

54. Plaintiff, individually and on behalf of the members of the California Class, also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

SECOND CAUSE OF ACTION

For Unlawful and Unfair Business Practices Under California Business and Professions Code § 17200, *et seq.*

55. Plaintiff incorporates the above allegations by reference.

56. Plaintiff brings this cause of action on behalf the California Class whose personal information was compromised as a result of the data breach publicized in February 2015.

57. Anthem's acts and practices, as alleged in this complaint, constitute unlawful and unfair business practices, in violation of the Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq*.

58. Anthem's acts and practices, as alleged in this complaint, constitute unlawful practices in that they violate California Civil Code section 1798.80, *et seq*., the Health Insurance and Portability and Accountability Act (HIPAA), and because Anthem's conduct was negligent.

a. California Civil Code section 1798.81.5(b): Anthem's practices were unlawful and in violation of California Civil Code section 1798.81.5(b) because Anthem failed to take reasonable security measures in protecting its former and current employees' personal data.

b. Anthem's practices were unlawful and in violation of California Civil Code section 1798.82 because Anthem has unreasonably delayed informing Plaintiff and members of the class about the breach of security after Anthem knew the data breach occurred.

c. Anthem violated HIPAA by failing to establish procedures to keep employees' medical information confidential and private. Protected health information under HIPAA includes "individually identifiable health information," including name, address, date of birth, and social security number. *See* United States Department of Health and Human Services, OCR Privacy Brief, *http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf*. The Department of Health and Human Services Office of Civil Rights issued a statement regarding the Anthem data breach, which noted that "[t]he personally identifiable information health plans maintain on enrollees and members — including names and social security numbers — is protected under HIPAA, even if no specific diagnostic or

treatment information is disclosed."[22] 45 C.F.R. § 164.530(c)(1) requires that health care provides implement reasonable safeguards for this information, which Anthem failed to do. 45 C.F.R. § 164.404 requires that companies provide notice of the breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons – i.e. non-encrypted data. *See* 45 C.F.R. § 164.402. Anthem has failed to provide such notice.

59. The acts, omissions, and conduct of Anthem also constitute a violation of the unlawful prong of the UCL because it failed to comport with a reasonable standard of care and public policy as reflected in statutes such as the Information Practices Act of 1977, California Customer Records Act, and HIPAA, which seek to protect individuals' data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

60. In failing to protect plan members' and employees' personal information and unduly delaying informing them of the data breach, Anthem has engaged in unfair business practices by engaging in conduct that undermines or violates the stated policies underlying the California Customer Records Act and the Information Practices Act of 1977. In enacting the California Customer Records Act, the Legislature stated that: "[i]dentity theft is costly to the marketplace and to consumers" and that "victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative." 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700) (WEST). Anthem's conduct also undermines California public policy as reflected in other statutes such as the Information Practices Act of 1977, Cal. Civ. Code § 1798, *et seq*., which seeks to protect individuals' data and ensure that

[22] Ricardo Alonso-Zaldivar, *Anthem Breach: A Gap in Federal Health Privacy Law*, ABC NEWS, http://abcnews.go.com/Politics/wireStory/anthem-breach-reveals-gap-federal-health-privacy-law-28781059 (last visited Feb. 8, 2015).

entities who solicit or are entrusted with personal data utilize reasonable security measures.

61. As a direct and proximate result of Anthem's unlawful and unfair business practices as alleged herein, Plaintiff and members of the class have suffered injury in fact. Plaintiff and the class have been injured in that their personal information has been compromised and they are at an increased risk for future identity theft and fraudulent activity on their financial accounts. Class members have also lost money and property by purchasing credit monitoring services they would not otherwise had to but for Anthem's unlawful and unfair conduct.

62. As a direct and proximate result of Anthem's unlawful and unfair business practices as alleged herein, Plaintiff and class members face an increased risk of identity theft and medical fraud, based on the theft and disclosure of their personal information.

63. Because of Anthem's unfair and unlawful business practices, Plaintiff and the class are entitled to relief, including restitution to Plaintiff and class members for costs incurred associated with the data breach and disgorgement of all profits accruing to Anthem because of its unlawful and unfair business practices, declaratory relief, and a permanent injunction enjoining Anthem from its unlawful and unfair practices.

64. The injunctive relief that Plaintiff and members of the class are entitled to includes, but is not limited to: (1) ordering that Anthem, 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 Anthem's systems on a periodic basis; (2) ordering that Anthem engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Anthem audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Anthem, consistent with industry standard practices, conduct regular database scanning and securing checks; (5) ordering that Anthem, 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; (6) ordering Anthem to meaningfully educate its former and current members and employees about the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves; and (7) ordering Anthem to encrypt sensitive personal information.

65. Plaintiff, individually and on behalf of the members of the class, also seeks reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

THIRD CAUSE OF ACTION

Breach of Contract

66. Plaintiff incorporates the above allegations by reference.

67. Plaintiff brings this cause of action on behalf of the Nationwide Class whose personal information was compromised as a result of the data breach publicized in February 2015.

68. Anthem's Personal Information Privacy Protection Policy promises 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 and Blue Shield is committed to protecting information about its customers and associates, especially the confidential nature of their personal information (PI)."[23] The policy also purports to "safeguard[] Social Security numbers and other personal information by having physical, technical, and administrative safeguards in place."[24]

69. Anthem's privacy policies constitute and agreement between (1) Anthem and (2) its health plan members and employees.

[23] Anthem Privacy Website, https://www.anthem.com/health-insurance/about-us/privacy (last visited Feb. 8, 2015).

[24] *Id.*

70. Anthem has breached its agreement with class members to protect their personal information by (1) failing to implement security measures designed to prevent this attack even though the health care industry has been repeatedly warned about the risk of cyber-attacks, (2) failing to employ security protocols to detect the unauthorized network activity, and (3) failing to maintain basic security measures such as complex data encryption so that if data were accessed or stolen it would be unreadable.

71. Plaintiff and class members have been damaged by Anthem's breach of its obligations because their personal information has been compromised and they are at and increased risk for future identity theft and fraudulent activity on their financial accounts. Class members have also lost money and property by purchasing credit monitoring services they would not otherwise had to but for Anthem's unlawful and unfair conduct

72. Plaintiff, individually and on behalf of the members of the California Class, seeks (a) damages suffered by members of the class, (b) equitable relief, and (c) injunctive relief requiring Anthem to implement safeguards consistent with its contractual promises.

73. Plaintiff, individually and on behalf of the members of the class, also seeks reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

FOURTH CAUSE OF ACTION

Negligence

74. Plaintiff incorporates the above allegations by reference.

75. Plaintiff brings this cause of action on behalf of the Nationwide Class whose personal information was compromised as a result of the data breach publicized in February 2015.

76. In collecting the personal information of its current and former health insurance plan members and employees, Anthem owed Plaintiff and members of the class a duty to exercise reasonable care in safeguarding and protecting that information. This duty included, among other things, maintaining and testing Anthem's security systems

and taking other reasonable security measures to protect and adequately secure the personal data of Plaintiff and the class from unauthorized access and use. Anthem's security system and procedures for handling the personal information of its current and former health insurance plan members and employees were intended to affect Plaintiff and the class. Anthem was aware that by taking such sensitive information of its health insurance plan members and employees, it had a responsibility to take reasonable security measures to protect the data from being stolen and, in the event of theft, easily accessed.

77. The duty Anthem owed to Plaintiff and members of the class to protect their personal information is also underscored by the California Customer Records Act and HIPAA, which recognize the importance of maintaining the confidentiality of personal information and were established to protect individuals from improper disclosure of their personal information.

78. Additionally, Anthem had a duty to timely disclose to Plaintiff and members of the class that their personal information had been or was reasonably believed to have been compromised. Timely disclosure is appropriate so that Plaintiff and members of the class could, among other things, report the theft of their Social Security numbers to the Internal Revenue Service, monitor their credit reports for identity fraud, undertake appropriate measures to avoid unauthorized charges on their debit card or credit card accounts, and change or cancel their debit or credit card PINs (personal identification numbers) to prevent or mitigate the risk of fraudulent cash withdrawals or unauthorized transactions.

79. There is a very close connection between Anthem's failure to take reasonable security standards to protect its current and former health insurance plan members' and employees' data and the injury to Plaintiff and the class. When individuals have their personal information stolen, they are at risk for identity theft, and need to buy credit monitoring services and purchase credit reports to protect themselves from identity theft.

80. Anthem is morally to blame for not protecting the data of its current and former health insurance plan members and employees by failing to take reasonable security measures. If Anthem had taken reasonable security measures, data thieves would not have been able to take the personal information of tens of millions of current and former Anthem health insurance plan members and Anthem employees.

81. The policy of preventing future harm weighs in favor of finding a special relationship between Anthem and the class. Anthem's health insurance plan members and employees count on Anthem as their health care provider and/or employer to keep their data safe and in fact are required to share sensitive personal data with Anthem as a condition of health plan enrollment and/or employment. If companies are not held accountable for failing to take reasonable security measures to protect their customers' and employees' personal information, they will not take the steps that are necessary to protect against future data breaches.

82. It was foreseeable that if Anthem did not take reasonable security measures, the data of Plaintiff and members of the class would be stolen. Major corporations, particularly those in the health care industry, like Anthem, face a higher threat of security breaches than other companies due in part to the large amounts and type of data they possess. Anthem should have known to take precautions to secure its health plan members' and employees' data, especially in light of recent data breaches and warnings regarding cyberattacks and network vulnerability in the health care industry.

83. Anthem breached its duty to exercise reasonable care in protecting the personal information of Plaintiff and the class by failing to implement and maintain adequate security measures to safeguard its health plan members' and employees' personal information, failing to monitor its systems to identify suspicious activity, allowing unauthorized access to the personal information of Plaintiff and the class, and failing to encrypt or otherwise prevent unauthorized reading of such personal information.

84. Anthem breached its duty to timely notify Plaintiff and the class about the data breach. Anthem has failed to issue any notice to its current and former health plan members and employees affected by the breach. Additionally, Anthem was, or should have been, aware of breaches in its network security as early as December 10, 2014.

85. But for Anthem's failure to implement and maintain adequate security measures to protect its current and former health plan members' and employees' personal information and failure to monitor its systems to identify suspicious activity, the personal information of Plaintiff and members of the class would not have been stolen, and they would not be at a heightened risk of identity theft in the future.

86. Anthem's negligence was a substantial factor in causing harm to Plaintiff and members of the class.

87. As a direct and proximate result of Anthem's failure to exercise reasonable care and use commercially reasonable security measures, the personal information of current and former Anthem health plan members and Anthem employees was accessed by unauthorized individuals who could use the information to commit identity fraud, medical fraud, or debit and credit card fraud. Plaintiff and the class face a heightened risk of identity theft in the future.

88. Members of the class have also suffered economic damages, including the purchase of credit monitoring services they would not have otherwise purchased.

89. Neither Plaintiff nor other members of the class contributed to the security breach, nor did they contribute to Anthem's employment of insufficient security measures to safeguard employees' personal information.

90. Plaintiff and the class seek compensatory damages and punitive damages with interest, the costs of suit and attorneys' fees, and other and further relief as this Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed classes, requests that the Court:

a. Certify this case as a class action on behalf of the classes defined above, appoint Aswad Hood as class representative, and appoint Girard Gibbs as class counsel;

b. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and other class members;

c. Award restitution and damages to Plaintiff and class members in an amount to be determined at trial;

d. Award Plaintiff and class members their reasonable litigation expenses and attorneys' fees;

e. Award Plaintiff and class members pre- and post-judgment interest, to the extent allowable; and

f. Award such other and further relief as equity and justice may require.

Dated: February 9, 2015

Respectfully Submitted,

GIRARD GIBBS LLP

By: */s/ Eric H. Gibbs*

Daniel C. Girard
Eric H. Gibbs
Scott M. Grzenczyk
Steven A. Lopez
GIRARD GIBBS LLP
601 California Street, 14th Floor
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
Email: dcg@girardgibbs.com

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: February 9, 2015

Respectfully Submitted,

GIRARD GIBBS LLP

By: /s/ Eric H. Gibbs

Daniel C. Girard
Eric H. Gibbs
Scott M. Grzenczyk
Steven A. Lopez
GIRARD GIBBS LLP
601 California Street, 14th Floor
San Francisco, California 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846
Email: dcg@girardgibbs.com