Richard D. McCune, State Bar. No. 132124
E-mail: rdm@mccunewright.com
David C. Wright, State Bar No. 177468
E-Mail: dcw@mccunewright.com
Michele M. Vercoski, State Bar No. 244010
E-mail: mmv@mccunewright.com
MCCUNEWRIGHT LLP
2068 Orange Tree Lane, Suite 216
Redlands, California 92374
Telephone: (909) 557-1250
Facsimile: (909) 557-1275

John A. Yanchunis, Florida State Bar No. 324681*
E-mail: JYanchunis@ForThePeople.com
Rachel Soffin, Florida State Bar No. 0018054*
E-mail: RSoffin@ForThePeople.com
MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, Florida, 33602
Telephone: (813) 223-5505
Facsimile: (813) 222-4738

Steven W. Teppler, Florida State Bar No. 14787*
E-mail: steppler@abbottlawpa.com
ABBOTT LAW GROUP P.A.
2929 Plummer Cove Road
Jacksonville, FL 32223
Telephone: (904) 292-1111
Facsimile: (904) 292-1220

Joel R. Rhine, NC State Bar No. 16028*
E-Mail: jrr@rhinelawfirm.com
RHINE LAW FIRM, P.C.
1612 Military Cutoff Road, Ste. 300
Wilmington, NC 28403
Telephone: (910) 777-7651
Facsimile: (910) 772-9062

Pro Hac Vice Applications to be submitted

Attorneys for Plaintiffs and the Putative Classes

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF LOS ANGELES

MIGUEL ORTIZ, on behalf of himself and all others similarly situated,

Plaintiff,

v.

UCLA HEALTH SYSTEM, a public entity; UCLA MEDICAL SCIENCES, a public entity; THE REGENTS OF THE UNIVERSITY OF CALIFORNIA, a public entity; and DOES 1 though 100, inclusive,

Defendants.

Case No.: BC 589327

CLASS ACTION COMPLAINT FOR INJUNCTIVE RELIEF:

1. Violation of California Customer Records Act (Civ. Code, §§ 1798.81.5, 1798.82);
2. Violation of the Confidentiality of Medical Information Act (Civ. Code, § 56, *et seq.*);
3. Violation of California Unfair Competition Law (Bus. & Prof. Code, § 17200);
4. Invasion of Privacy
5. Negligence

PLAINTIFF'S CLASS ACTION COMPLAINT

Plaintiff MIGUEL ORTIZ ("Plaintiff") brings this action against Defendants UCLA HEALTH SYSTEM, UCLA MEDICAL SCIENCES, the REGENTS OF THE UNIVERSITY OF CALIFORNIA, and Does 1-100 by and through his attorneys, individually and on behalf of all others similarly situated ("Class"), and alleges as follows:

INTRODUCTION

1. On or about September 2014, Plaintiff's and Class members' personally identifiable information ("PII") and other highly sensitive information was stolen from Defendants UCLA HEALTH SYSTEM, UCLA MEDICAL SCIENCES (hereinafter "UCLA HEALTH"), the REGENTS OF THE UNIVERSITY OF CALIFORNIA (hereinafter "Regents"), and Does 1-100 (collectively "Defendants"), as a result of Defendants' negligence and failure to take reasonable steps to keep the information secure.

2. Based on information and belief, Defendants were specifically targeted by cybercriminals because of the PII it housed for millions of customers has tangible value on the black market. The information that was stolen includes the most intimate details of Plaintiff's and Class members' lives, including their Social Security numbers, birth dates, medical records, financial information, addresses, and the like. Such information is particularly vulnerable to attack by cyber criminals, because it is the type of information that is easily utilized for identity theft and credit fraud.

3. Defendants knew that the information was a likely target for attack by cyber criminals given their prior history of being hacked, and the host of highly publicized massive data breaches that have recently been aimed at health care and other industries. Despite this knowledge, they did not take adequate steps to safeguard the information.

4. Defendants, who provided healthcare services to Plaintiff and Class members, owed a duty of care to Plaintiff and Class members in the acquisition and retention of their PII. Defendants breached this duty by failing to invest in adequate security and by failing to take even the most basic steps in protecting the information, such as encrypting the information, despite Defendants' general knowledge of the dangers of theft of PII, and Defendants' specific knowledge of their susceptibility to the theft of PII that came from their own loss of patient information to hackers in approximately 2006.

5. Moreover, once learning of the breach of the PII, Defendants failed to promptly notify Plaintiff and Class members of the theft. Instead, despite first learning of a probable breach in September 2014, Defendants waited more than eight months to notify Plaintiff and putative Class members that their highly sensitive personal information had been stolen. Then, when apparently positively confirming the extent and specifics of the breach in May 2015, Defendants still waited almost sixty days to notify Plaintiff and the putative class of the breach of their PII data. Even now, Defendants continue to withhold information to Plaintiff and the Class members as to the specifics of who accessed their information, when that PII was stolen, and precisely what PII information was stolen.

6. The risk that Plaintiff's and the Class members' data will be misappropriated by the hackers who breached Defendants' network is immediate and real. Because of this immediate and real threat, Plaintiff and the Class members will spend time and money to protect themselves from that threat. As the specific result of Defendants' conduct, Plaintiff and Class members, as well as their family members, will spend time and money in monitoring their credit scores and credit accounts because of the high likelihood that the stolen data will be used for fraudulent purposes. Further, because the stolen information contains medical insurance information, there is a high likelihood that information will be used for fraudulent or illegal purposes that can have not only financial implications, but even more serious health implications. Plaintiff and the Class members will spend time and money in monitoring their medical insurance and health information to verify that the medical bills, payments, treatment, and diagnosis relates to them, and not someone using their medical information for fraudulent purposes. Plaintiff and Class members have also suffered and will continue to suffer an invasion of privacy as a consequence of their private information, including medical records, having been stolen, viewed, and used by others.

7. Defendants' acts and omissions violated the Customer Records Act (Civ. Code, § 1798.80, *et seq.*); the Confidentiality of Medical Information Act (Civ. Code, § 56, *et seq.*); Unfair Competition Law (Civ. Code, § 17200); and common law invasion of privacy.

8. Plaintiff seeks, on behalf of himself and the putative Class members, appropriate injunctive relief requiring Defendants to comply with their legal obligations, as well as additional and

further relief that may be appropriate. Plaintiff reserves the right to amend the Complaint to add additional relief, including but not limited to damages, as permitted under applicable law.

JURISDICTION

9. The Court has personal jurisdiction over Defendants because Defendants UCLA HEALTH SYSTEM's and UCLA MEDICAL SCIENCES' principal place of business is located in Los Angeles, California, and Defendant THE REGENTS OF THE UNIVERSITY OF CALIFORNIA is and was a public entity of the State of California existing pursuant to the California Constitution, Article IX, Section 9.

10. Venue is proper in this county because Plaintiff resides in the county and Defendants UCLA HEALTH SYSTEM and UCLA MEDICAL SCIENCES are public entities headquartered in Los Angeles County, and/or because this county is the county in which a substantial part of the events or omissions giving rise to the improper conduct alleged herein occurred.

PARTIES

11. Plaintiff MIGUEL ORTIZ is a citizen and resident of Los Angeles, California.

12. Upon information and belief, Defendant UCLA HEALTH SYSTEM and UCLA HEALTH SCIENCES are public entities doing business in California, with their headquarters in Los Angeles, California. Based on information and belief, these Defendants own, maintain or control at least four hospitals and 150 medical offices across Southern California.

13. Upon information and belief, Defendant THE REGENTS OF THE UNIVERSITY OF CALIFORNIA is a public entity doing business throughout the State of California.

14. The true names and capacities of the defendants sued herein as Does 1 through 100, inclusive, are currently unknown to Plaintiff, who therefore sues such defendants by such fictitious names. Each of the defendants designated herein as a Doe is legally responsible in some manner for the unlawful acts referred to herein. Plaintiff will seek leave of Court to amend this complaint to reflect the true names and capacities of the defendants designated herein as Does when such identities become known.

15. Based upon information and belief, Plaintiff alleges that at all times mentioned herein, each and every Defendant was acting as an agent and/or employee of each of the other Defendants, and

at all times mentioned was acting within the course and scope of said agency and/or employment with the full knowledge, permission, and consent of each of the other defendants. In addition, each of the acts and/or omissions of each Defendant alleged herein were made known to, and ratified by, each of the other Defendants.

FACTUAL ALLEGATIONS

16. As leaders in the health care industry, assisting millions of Californians in their healthcare needs, Defendants are in the business of maintaining their patients' most private information.

17. In or about 2011, Plaintiff ORTIZ began visiting UCLA Health Center as a patient for all of his and his family's primary medical care needs. During his multiple visits as a patient with UCLA HEALTH, Plaintiff ORTIZ provided his non-public personal information, medical history, and medical information to Defendants, who used it for medical diagnosis, treatment, prescriptions and other highly private uses.

18. Based on information and belief, on or before September 2014, Defendants became aware that unknown persons had improperly accessed and stolen PII from their system that stores approximately 4.5 million of UCLA HEALTH's current and former customers' highly sensitive personal and health information, including, but not limited to, Social Security numbers, birth dates, medical records, financial information, addresses, and health insurance account numbers.

19. Despite becoming aware that their system had been hacked and that Plaintiff's and Class members' private information was stolen, Defendants did not promptly make the fact of the data breach public or notify their patients.

20. Instead, Defendants waited more than eight months before acknowledging the theft. Not until July 17, 2015, did they announce, for the first time, that their current and former patients' highly personal information had been stolen.

21. The theft was the result of Defendants' failure to take adequate security measures to safeguard the information. Defendants, as health care providers, are legally required to keep their patients' PII protected. Nevertheless, Defendant failed to take even the most basic precautions such an encrypting Plaintiff's and Class members' PII.

22. Defendants' failure to take the necessary steps to safeguard their patients' extremely sensitive personal data is even more troublesome in light of the recent surge in massive data breaches experienced by large corporations such as Home Depot, Chase Bank, Target, Sony, Premera Blue Cross, and Anthem Blue Cross. As a result of these massive data breaches, Defendants should have known that their patients' personal data was at great risk of being stolen and used for fraudulent purposes by cybercriminals.

23. Over the past year alone, millions of people have fallen prey to identity theft through massive data breaches at some of the nation's largest companies. The following are examples of the largest data breaches in recent times:

a. In September 2014, Home Depot, the world's largest home improvement chain, confirmed that a total of 56 million credit and debit cards were affected by a data breach;

b. In June and July 2014, JP Morgan Chase, the nation's largest bank by assets, confirmed that it had experienced a massive data breach that affected 76 million households and 7 million small businesses;

c. In early December 2014, Sony's system was hacked, resulting in the theft of 47,000 social security numbers, which subsequently appeared more than 1.1 million times on 601 publicly-posted files stolen by hackers;

d. In January 2014, it was revealed that Target Corporation's holiday data breach affected up to 70 million people, who had their names, mailing addresses, phone numbers, and email addresses stolen by hackers;

e. In January 2015, it was revealed that health insurance giant Premera Blue Cross experienced a data breach involving the personal data of approximately 80 million members across the country.

f. In February 2015, Anthem, Inc., the country's second largest health insurer, announced that its systems had been compromised in a massive data breach, in which a total of 78.8 million records were stolen, including 8.8 to 18.8 million records of non-customers.

g. In June 2015, the United States Office of Personnel and Management announced that its systems housing employee records had been breached by cybercriminals, resulting in a loss of sensitive data for approximately 14 million employees.

24. Defendants knew or should have known that Plaintiff's and Class members' private information had a high risk of being stolen. The type of sensitive personal, financial and medical data retained by Defendants is particularly targeted and sought after by identity thieves. The PII stolen by hackers has objective value on the black market because of the ability of criminals to use the stolen data for financial gain in ways that would damage and harm Plaintiff and the Class members.

25. Despite the increase in massive data breaches in recent times, and the nature of the information retained by Defendants, Defendants failed to implement reasonable cyber security measures. Defendants' failure to implement such measures allowed cybercriminals easier access to customers' personal data.

26. Defendants also should have known that theft of such highly personal information would have dire consequences, and in fact has had dire consequences, for Plaintiff and Class members. Not only have Plaintiff and Class members suffered an invasion of their privacy, they will have to be diligent and will expend out-of-pocket money for the rest of their lives in order to protect themselves against identity theft and credit fraud.

CLASS ALLEGATIONS

27. Plaintiff brings this action pursuant to Code of Civil Procedure section 382 on behalf of the following Class:

> **All current and former patients of Defendants that reside in California and whose personal information was housed on the UCLA Health network system that was accessed by cyber criminals.**

28. Excluded from the Class are Defendants' management employees, as well as the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change, or expand the Class definition.

29. ***Numerosity.*** The Class is so numerous that joinder of all members is impracticable. Upon information and belief, there are at least tens of thousands of individuals whose PII has been

stolen from Defendants. These individuals are identifiable from Plaintiff's description of the Class, from Defendants' records, and/or from the records of third parties accessible through discovery.

30. ***Typicality.*** Plaintiff's claims are typical of the claims of the Class. Plaintiff is a member of the Class he seeks to represent. All members of the Class, including Plaintiff, were and are similarly affected by Defendants' actions or omissions regarding the breach of personal and health information and the delay in disclosure of the breach in data, and the relief sought herein is for the benefit of Plaintiff and Class members.

31. ***Adequacy.*** The representative Plaintiff will fairly and adequately represent the members of the Class and has no interests that are antagonistic to the claims of the Class. Plaintiff's interests in this action are antagonistic to the interests of Defendants, and he will vigorously pursue the claims of the class. The representative Plaintiff has retained counsel who are competent and experienced in consumer class action litigation, and have successfully represented consumers in complex class actions.

32. ***Common Questions Predominate.*** There are numerous and substantial questions of law or fact common to all members of the Class that will predominate over any individual issues, including but not limited to:

a. Whether Defendants had a legal duty to use reasonable security measures to protect former and current patients' personal and medical information;

b. Whether Defendants breached their legal duty by failing to protect former or current patients' personal and medical information;

c. Whether Defendants promptly and reasonably investigated and notified Plaintiff and the Class members that their information had been compromised and assessed;

d. Whether Plaintiff and Class members are entitled to injunctive relief;

e. Whether Defendants violated Civil Code section 1798.81.5 by failing to implement reasonable security procedures and practices;

f. Whether Defendants violated Civil Code section 1798.82 by failing to promptly notify Class members that their personal information had been compromised;

g. Whether Defendants violated Civil Code section 56.20 by failing to maintain the confidentiality of Class members' medical information;

h. Whether Class members may obtain declaratory and injunctive relief against Defendants under Civil Code sections 1798.84, 56, or under the UCL;

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

33. ***Superiority.*** A class action is superior to other available methods for the fair and efficient adjudication of this controversy and would provide substantial benefits to both the courts and litigants. Arguably, no Class member could afford to seek legal redress individually for the claims alleged herein. Therefore, absent a class action, the Class members will continue to suffer losses and Defendants' misconduct will proceed without remedy. Even if Class members themselves could afford such individual litigation, the court system could not. Given the complex legal and factual issues involved, and considering that the Class could number in the tens of thousands or greater, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a class action presents far fewer management difficulties, allows claims to be heard which may otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION

VIOLATION OF CALIFORNIA'S CUSTOMER RECORDS ACT

(Civ. Code, § 1798.80, *et seq*)

34. Plaintiff and the Class incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

35. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Civil Code section 1798.81.5, which requires 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."

36. Defendants are a "business" within the meaning of Civil Code section 1798.80(a).

37. Plaintiff and members of the Class are "individual[s]" within the meaning of Civil Code section 1798.80(d).

38. Pursuant to Civil Code sections 1798.80(e) and 1798.81.5(d)(1)(C), the data theft included the theft of "personal information" as meant by those sections, including names, addresses,

Social Security numbers, driver's license or state identification card numbers, debit and credit card information, medical information, or health insurance information.

39. The breach of personal data of thousands of former or current patients of Defendants' constituted a "breach of the security system" of Defendants, under Civil Code section 1798.82(g).

40. By failing to implement reasonable measures to protect its former and current patients' personal and medical data, Defendants violated Civil Code section 1798.81.5.

41. In addition, by failing to promptly notify all affected former and current patients of Defendants that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the data breach, Defendants violated Civil Code section 1798.82 of the same title. Defendants' failure to timely notify patients of the beach has caused Class members damages because they had to take measures to remediate the breach caused by Defendants' negligence.

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

43. Accordingly, Plaintiff and the Class request that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures to protect patients' data in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (2) ordering that Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures; (4) ordering that Defendants purge, delete, and destroy in a reasonable secure manner patient data not necessary for their business/health care operations; (5) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning, real-time network traffic analysis, and security checks; (6) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (7) ordering Defendants to meaningfully educate their former and current

patients 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 (8) ordering Defendants to implement a written policy for implementation of the items (1) through (7), above.

44. Plaintiff further requests that the Court require Defendants 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 patients of any future data breaches by email within 24 hours of Defendants' discovery of a breach or possible breach.

45. As a result of Defendants' violation of Civil Code sections 1798.81.5 and 1798.82, Plaintiff, individually and on behalf of the members of the Class, seeks remedies under Civil Code section 1798.84, specifically, equitable relief.

46. Plaintiff, individually and on behalf of the members of the Class, also seeks reasonable attorney's fees and costs under applicable law, including Code of Civil Procedure section 1021.5.

SECOND CAUSE OF ACTION

VIOLATION OF THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT

(Civil Code, § 56, *et seq.*)

47. Plaintiff and the Class incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

48. Plaintiff brings this cause of action on behalf of the Class whose personal and medical information are maintained by Defendants and/or were released in the data breach.

49. California's Confidentiality of Medical Information Act (CMIA),Civ. Code, § 56, *et seq.*, requires Defendants, who are providers of health care services within a network of hospitals and offices that span throughout Southern California, to protect their patients' confidential medical information and to not release private medical information without signed proper authorization.

50. Plaintiff and the Class members are "patients" of Defendants within the meaning of Civil Code section 56.05(g). Furthermore, Plaintiff and the Class members, as patients of Defendants, had their personal medical information recorded and stored within Defendants' network.

51. Defendants requested and came into possession of Plaintiff's and Class members' personal and medical information and had a duty to exercise reasonable care in preserving the confidentiality of this information.

52. Defendants were entrusted with Plaintiff's and Class members' personal and medical information as providers of medical data processing and/or other administrative services, and therefore owed a duty of reasonable care to Plaintiff and Class members to preserve the confidentiality of their personal and medical information.

53. Under California Civil Code section 56.10, Defendants were required to obtain Plaintiff's and Class members' authorization prior to disclosing their personal or medical information.

54. On or before September 2014, Defendants negligently and unlawfully disclosed Plaintiff's and Class members' personal and medical information, without first obtaining Plaintiff's and Class members' authorization, when cyber hackers accessed Defendants' computer networks containing unencrypted and unprotected sensitive patient and subscriber information. Thus, Defendants' negligence constitutes a violation of Civil Code sections 56.10, 56.104, and 56.11.

55. As a result of the data breach, Plaintiff's and Class members' personal and medical information has been illegally obtained. Among other things, Defendants are and were negligent in failing to maintain their former and current patients' medical information in encrypted form; failing to use reasonable security procedures to prevent unauthorized access to files containing the medical information; failing to use reasonable authentication procedures so that the medical information could be tracked in case of a security breach; and by delaying the notification of their former and current patients that their private medical information had been compromised. All of these acts and omissions violated the CMIA and Health Insurance Portability and Accountability Act (HIPAA).

56. On behalf of himself and the Class members, Plaintiff seeks an order requiring Defendants to cease their violations of the CMIA. Among other things, Defendants should be required to stop negligently handling their patients' medical information and institute reasonable security procedures to protect their medical information in compliance with the CMIA, including, but not limited to: (1) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including

simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (2) ordering that Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures; (4) ordering that Defendants purge, delete, and destroy in a reasonable secure manner patient data not necessary for their business/health care operations; (5) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning, real-time network traffic analysis, and securing checks; (6) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (7) ordering Defendants to meaningfully educate their former and current patients 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 (8) ordering Defendants to implement a written policy for implementation of the items (1) through (7), above.

57. Plaintiff further seeks reasonable attorneys' fees and costs under applicable law, including Code of Civil Procedure section 1021.5.

THIRD CAUSE OF ACTION

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAWS

(Bus. & Prof. Code, § 17200)

58. Plaintiff and the Class incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

59. Plaintiff brings this cause of action on behalf of Plaintiff and the Class members whose personal and/or medical information was compromised as a result of the data breach.

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

61. Defendants' acts and practices, as alleged in this complaint, constitute unlawful and unfair practices in that they violate Civil Code section 1798.80, *et seq.,* the CMIA, the HIPPA, and because Defendants' conduct was negligent.

62. Defendants' practices were unlawful and in violation of Civil Code section 1798.81.5(b) because Defendants failed to take reasonable security measures in protecting their former and current patients' personal and health care data.

63. Defendants' practices were also unlawful and in violation of Civil Code section 1798.82 because Defendants unreasonably delayed informing Plaintiff and members of the Class about the breach of security after Defendants knew that the data breach occurred.

64. Defendants' practices were unlawful and in violation of section 56.20 of the CMIA because they did not establish proper procedures to secure the confidentiality of their former and current patients' medical information.

65. Defendants' practices were also unlawful and in violation of section 56.36(b) of the CMIA by negligently releasing Plaintiff's and Class Members' medical information that was within Defendants' control.

66. Defendants further violated the HIPAA by failing to establish procedures to keep patients' medical information confidential and private.

67. The acts, omissions, and conduct of Defendants constitute a violation of the unlawful prong of the UCL because they failed to comport with a reasonable standard of care and public policy as reflected in statutes such as the Information Practices Act of 1977, Civ. Code, § 1798, *et seq.,* HIPPA, and the California Customer Records Act, Civ. Code, § 1798.80, *et seq.,* which seek to protect individuals' data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

68. Defendants violated the "unfair" prong of the UCL because their acts and/or omissions were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class members, and because their acts and/or omissions constitute conduct that undermines or violates the stated policies underlying the California Customer Records Act and other privacy statutes. In enacting the California Customer Records Act, the Legislature state 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).) Defendants'

conduct also undermines California public policy as reflected in other statutes such as the Information Practices Act of 1977, Civ. Code, § 1798, *et seq.,* which seeks to protect individuals' data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

69. As a direct and proximate result of Defendants' unlawful business practices as alleged herein, Plaintiff and members of the Class have suffered the following injuries in fact and losses of money or property: (1) loss of opportunity to control how their PII is used; (2) diminution in the value and/or use of their PII; (3) the compromise, publication, and/or theft of their PII; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft or unauthorized use of financial and medical costs; (5) lost opportunity costs and loss of productivity from efforts to mitigate the actual and future consequences of the theft of PII; (6) cost associated with the inability to use credit and assets frozen or flagged as a result of credit misuse; (7) unauthorized use of compromised PII; (8) tax fraud or other unauthorized charges to financial, health care, or medical accounts; (9) continued risk to PII that remain in the possession of Defendants, as long as Defendants fail to undertake adequate measures to protect PII; and (10) future costs in terms of time, effort, and money that will be expended to prevent and repair the impact of the data breach.

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

71. As a result of Defendants' violations, Plaintiff and members of the Class are entitled to injunctive relief, including, but not limited to: (1) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (2) ordering that Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures; (4) ordering that Defendants purge, delete, and destroy in a reasonable secure manner patient data not necessary for their business/health care operations; (5) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning, real-time

network traffic analysis, and securing checks; (6) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (7) ordering Defendants to meaningfully educate their former and current patients 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 (8) ordering Defendants to implement a written policy for implementation of the items (1) through (7), above.

72. Because of Defendants' unfair and unlawful business practices, Plaintiff and the Class are entitled to relief, including (1) restitution to Plaintiff and Class members of the losses they incurred as a result of the data breach and restitutionary disgorgement of all profits accruing to Defendants as a result of their unlawful and unfair business practices; (2) attorneys' fees and costs; (3) declaratory relief; and (4) a permanent injunction enjoining Defendants from their unlawful and unfair practices.

FOURTH CAUSE OF ACTION

INVASION OF PRIVACY

73. Plaintiff and the Class incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

74. Defendants invaded Plaintiff's and the Class members' right to privacy by allowing the unauthorized access to Plaintiff's and Class members' PII and by negligently maintaining the confidentiality of Plaintiff's and Class members' PII, as set forth above.

75. The intrusion was offensive and objectionable to Plaintiff, the Class members, and to a reasonable person of ordinary sensibilities in that Plaintiff's and Class members' PII was disclosed without prior written authorization of Plaintiff and the Class.

76. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff's and the Class members' provided and disclosed their PII to Defendants, as patients of Defendants, privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class members were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

77. As a proximate result of Defendants' above acts, Plaintiff's and the Class members' PII was viewed, printed, distributed, and used by persons without prior written authorization and Plaintiff and the Class members suffered damages.

78. Defendants are guilty of oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiff's and the Class members' personal medical information with a willful and conscious disregard of Plaintiff's and the Class members' right to privacy.

79. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause Plaintiff and the Class members great and irreparable injury in that the PII maintained by Defendants can be viewed, printed, distributed, and used by unauthorized persons. Plaintiff and Class members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class.

FIFTH CAUSE OF ACTION

NEGLIGENCE

80. Plaintiff and the Class incorporate by reference each preceding and succeeding paragraph as thought fully set forth at length herein.

81. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting Plaintiff's and Class members' personal information and taking reasonable measures to prevent their personal information from being compromised, lost, stolen, accessed, and misused by unauthorized persons. This duty included, among other things, designing, implementing, maintaining, and testing Defendants' security systems and protocols, consistent with industry standards and requirements, to ensure that Plaintiff's and Class members' PII in Defendants' possession was adequately secured and protected. Defendants further owed a duty to Plaintiff and Class members to implement processes that would detect a breach of their security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

82. Defendants owed a duty of care to Plaintiff and Class members because they were foreseeable and probable victims of Defendants' inadequate security practices. Defendants solicited, gathered, and stored the personal data provided by Plaintiff and Class members in the regular course of

their business. Defendants knew that they inadequately safeguarded such information on their computer systems. Defendants knew that a breach of its systems would cause damages to Plaintiff and Class members, and Defendants had a duty to adequately protect such sensitive PII.

83. Similarly, Defendants owed a duty to Plaintiff and Class members to timely disclose any incidents of data breaches, where such breaches compromised the PII of Plaintiff and Class members. Plaintiffs and Class members were foreseeable and probable victims of any inadequate notice practices. Defendants knew that, through their actions and omissions, they contributed to the theft of the PII of Plaintiff and Class members, and that the thieves manifested an intent to do harm to Plaintiff and Class members. Such harm could only be mitigated by timely notice of the theft.

84. Defendants breached their duties owed to Plaintiff and Class members by: (1) failing to exercise reasonable care in the adoption, implementation, and maintenance of adequate IT security procedures, infrastructure, personnel, and protocols; and (2) failing to timely notify Plaintiff and Class members of the data theft.

85. Defendants' breach of its duties owed to Plaintiff and Class members caused injuries to Plaintiff and Class members including, but not limited to: (1) theft of their PII; (2) costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts and medical records; (3) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the data theft including, without limitation, finding fraudulent charges, cancelling and reissuing credit cards and bank accounts, purchasing credit monitoring and identity theft protection, and the stress, nuisance and annoyance of dealing with all issues resulting from the data theft; (4) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by the data theft; (5) damages to and diminution in value of their PII entrusted to Defendants for the purpose of deriving health care from Defendants and with the understanding that Defendants would safeguard their data against theft and not allow access and misuse of their data by others; and (6) the continued risk to their PII, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect data in their possession.

86. But for Defendants' negligent and wrongful breach of their duties owed to Plaintiff and the Class, Plaintiff and the Class would not have been harmed and could have taken remedial measures to protect their PII.

87. Plaintiff and Class members seek injunctive and declaratory relief. Plaintiff and the Class reserve their right to seek damages and other relief as may be appropriate.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and members of the Class, respectfully requests that this Court:

A. Certify this case as a class action on behalf of the Class defined above, appoint Miguel Ortiz as class representative, and appoint his counsel as Class Counsel;

B. Award declaratory and equitable relief as is necessary to protect the interests of Plaintiff and the Class members;

C. Award Plaintiff and the Class members their reasonable litigation expenses and attorneys' fees;

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

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

Dated: July 29, 2015

Respectfully submitted,
MCCUNEWRIGHT LLP

By: _____
Richard D. McCune
Attorneys for Plaintiffs and Putative Classes