Danielle L. Perry (SBN 292120)
Gary E. Mason
Whitfield Bryson & Mason LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Phone: 202-640-1168
Fax: 202-429-2294
dperry@wbmllp.com

Attorneys for Plaintiff

[Additional counsel to appear on signature page]

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

JEANINE ST. HILL, individually and on behalf of others similarly situated,

Plaintiff(s),

v.

CENTRELAKE MEDICAL GROUP, INC., a Professional Corporation, aka Centrelake Imaging & Oncology,

Defendant(s).

CASE NO.

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff, JEANINE ST. HILL, individually, and on behalf of all others similarly situated, brings this action against Defendant, CENTRELAKE MEDICAL GROUP, INC., a California Professional Corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record:

JURISDICTION AND VENUE

1. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1332 & 1367 because this is a class action in which the matter or controversy exceeds the sum of $5,000,000, exclusive of interest and costs, and in which at least one member of the proposed class is a citizen of a state different from Defendant.

2. This Court has personal jurisdiction over Defendant because Defendant transacts business in this District, in the State of California, within the United States, and has contacts with this District sufficient to subject it to personal jurisdiction.

3. In accordance with 28 U.S.C. § 1391, venue is proper in this District because a substantial portion of the events or omissions giving rise to this action occurred in this District, and the Data Breach (as defined below) affected consumers in this District.

NATURE OF THE ACTION

4. Plaintiff brings this class action against Defendant for failing to secure and safeguard the personally identifiable information ("PII") and protected health information ("PHI") that Defendant collected and maintained (collectively, the "Private Information"), and for failing to provide timely and adequate notice to Plaintiff and other Class members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed (the "Data Breach").

5. Due to Defendant's negligence, the Private Information that Defendant collected and maintained could now be in the hands of thieves. Accordingly, Plaintiff brings this action

against Defendant seeking redress for its unlawful conduct asserting claims for violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq.*, violation of California's Unfair Competition Law, Cal Bus. & Prof. Code § 17200, *et seq.*, negligence, an intrusion upon seclusion, violation of Plaintiff and Class members' California Constitutional right to privacy, violation of California's Consumers Legal Remedies Act, and breach of express and implied contract.

PARTIES

6. Plaintiff, Jeanine St. Hill, is and at all times mentioned herein was, an individual citizen of the State of California residing in Ontario, California.

7. Defendant, Centrelake Medical Group, Inc. (hereinafter, "Defendant" or "Centrelake") is a California Professional Corporation within the meaning of Title 1, Division 3, Part 4 of the California Corporations Code with its principal place of business in Covina, California.

CENTRELAKE'S BUSINESS

8. Defendant operates a network of eight (8) outpatient radiology centers in California with locations in El Monte, Chino, Downey, Covina, Ontario, Pomona, Upland, and West Covina.

9. Defendant offers a comprehensive range of outpatient radiology services as well as various radiation therapy procedures.

10. In the ordinary course of receiving treatment and health care services from Defendant, patients provide Defendant with personal information such as:

- Name, address, phone number and email address;
- Information relating to individual medical history;
- Insurance information and coverage;
- Information concerning an individual's doctor, nurse or other medical providers; and
- Other information that may be deemed necessary to provide care.

11. Defendant also gathers certain medical information about patients and creates a record of the care it provides to patients.

12. Additionally, Defendant may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care", such as referring physicians, patient's other doctors, patient's health plan, close friends, or family members.

13. All of Defendant's employees, staff, entities, sites, and locations may share patient information with each other for various purposes as disclosed in the Centrelake Imaging and Oncology Notice of Privacy Practices.[1]

14. Upon information and belief, patients are provided with Defendant's Notice of Privacy Practices prior to service being rendered by Defendant.

15. Because of the highly sensitive and personal nature of the information Defendant acquires and stores in respect to its patients, Defendant promises to: (1) maintain the privacy of medical information provided; (2) provide notice of its legal duties and privacy practices; and (3) abide by the terms of its Notice of Privacy Practices currently in effect.

THE DATA BREACH

16. Plaintiff brings this suit individually and on behalf of a class of similarly situated individuals against Defendant for Defendant's failure to secure and protect Plaintiff and Class members' Private Information.

17. On April 16, 2019, Defendant issued a press release acknowledging that on January 9, 2019 an unknown third-party gained access to certain servers on Defendant's information system.[2]

18. According to Defendant, they became aware of the Data Breach on February 19, 2019 when a computer 'virus' prohibited Defendant from accessing its own files.

[1] https://centrelakeimaging.com/themes/igws/assets/pdf/privacypolicy.pdf
[2] https://centrelakeimaging.com/themes/igws/assets/pdf/press-release-4.16.19-1.pdf

19. Defendant launched an investigation and worked to restore its information systems with the assistance of a third-party forensics team.

20. The investigation determined that the virus had been introduced by an unknown third-party who had gained access to certain servers on Defendant's information system beginning as early as January 9, 2019.

21. The investigation confirmed that the servers, that were accessed by the third-party, contained information which might include patients' names, addresses, phone numbers, Social Security numbers, services performed with diagnosis information, driver's license information, health insurance information, referring provider information, medical record number, and dates of service.

22. Defendant's press release, dated April 16, 2019, states, in the present tense, that "Centrelake is providing notification to impacted patients . . ."[3]

23. On information and belief, and in light of Defendant's information-sharing policies in respect to its various sites and entities, the servers that were accessed contained Private Information for patients from all eight of Defendant's locations.

24. On information and belief, the Private Information accessed by the unknown third-party pertained to both adults and children.

25. What's more, Defendant's press release still does not indicate that Defendant has properly secured its information systems, or the computerized data contained therein which stores the Private Information of Plaintiff and the Class members.

26. According to Defendant's press release, Defendant's investigation is 'ongoing'.

27. Defendant specifically acknowledged the heightened risk of identity theft and fraud associated with the Data Breach in question in its April 16, 2019 press release by stating: "Centrelake encourages affected individuals to remain vigilant against incidents of identity theft

[3] *Id.*

and fraud and to seek to protect against possible identity theft or other financial loss by regularly reviewing their financial account, statements, credit reports, and explanations or benefits for suspicious activity."[4]

28. Defendant's call for vigilance, conveyed to affected individuals via its press release, did not come until almost two months after it discovered the breach, and more than three months after the onset of the breach.

DATA BREACHES PUT CONSUMERS AT

AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

29. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[5]

30. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[6]

31. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

32. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's

---

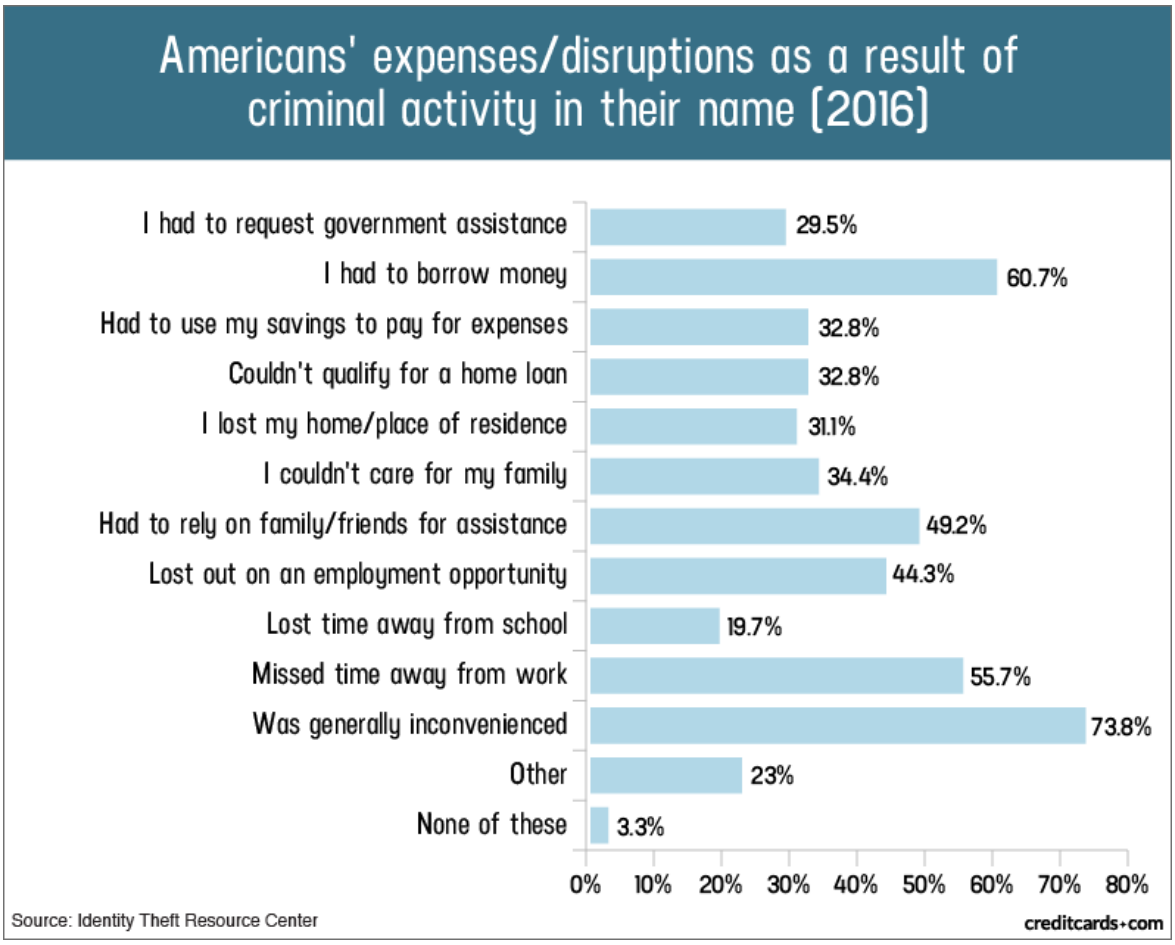
[4] *Id.*

[5] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").

[6] *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).

name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

33. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:



Source: "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited June 20, 2019).

34. What's more, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.[7] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

35. Theft of PHI, in particular, is gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[8] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

36. It must also be noted there may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that

[7] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[8] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited March 27, 2014).

information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

37. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

38. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

PLAINTIFF AND CLASS MEMBERS' DAMAGES

39. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

40. Plaintiff and Class members have suffered or will suffer actual injury as a direct result of the Data Breach. In addition to fraudulent charges, loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts, and damage to their credit, many victims suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Contacting their financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

41. Moreover, Plaintiff and Class members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

42. Further, as a result of Defendant's conduct, Plaintiff and Class members are forced to live with the anxiety that their private health information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

43. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ALLEGATIONS

44. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("the Class").

45. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All individuals whose Private Information was received, gatherer, shared, obtained, or otherwise found itself in the possession of Centrelake Medical Group, Inc. and compromised in the Data Breach. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

46. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, the Class may approach 197,661 patients.[9]

47. Commonality. Fed. R. Civ. P. 23(a)(2) & (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff and Class members' Private Information;

b) Whether Defendant unreasonably delayed in notifying affected customers of the Data Breach and whether the belated notice was adequate;

c) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

[9] https://www.databreaches.net/centrelake-medical-group-notifies-patients-after-ransomware-investigation-reveals-earlier-intrusion-and-suspicious-activity/

d) Whether Defendant's conduct was negligent;

e) Whether Defendant violated the requirements of Cal. Civ. Code § 1798.80, *et seq.*;

f) Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia;

g) Whether Defendant's acts, inactions, and practices complained of herein violated Plaintiff and Class members' California Constitutional Right to Privacy;

h) Whether Defendant's acts, inactions, and practices complained of herein violated California Consumers Legal Remedies Act; and

i) Whether Plaintiff and Class members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

48. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class members because Plaintiff's information, like that of every other Class member, was misused, and/or disclosed by Defendant.

49. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

50. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all Class members is impracticable. Furthermore, the adjudication of this controversy through a

class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

51. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

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

CAUSES OF ACTION

FIRST COUNT

Violation of the California Confidentiality of Medical Information Act

(Cal. Civ. Code § 56, *et seq.*)

(On Behalf of Plaintiff and All Class Members)

53. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

54. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization."

55. At all relevant times, Defendant was a health care provider because it had the "purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis or treatment of the individual." Cal. Civ. Code 6 § 56.06(a).

56. At all relevant times, Defendant collected, stored, managed, and transmitted Plaintiff and Class members' PII/PHI.

57. The CMIA requires Defendant to implement and maintain standards of confidentiality with respect to all individually identifiable PHI disclosed to them and maintained by them. Specifically, Cal. Civ. Code § 56.10(a) prohibits Defendant from disclosing Plaintiff and Class members' PHI without first obtaining their authorization to do so.

58. Section 56.11 of the California Civil Code specifies the manner in which authorization must be obtained before PHI is released. Defendant, however, failed to obtain any authorization—let alone, proper authorization—from Plaintiff and Class members before releasing and disclosing their PHI. Defendant also failed to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and Class members' PHI as required by California law. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff and Class members' PHI was disclosed. By disclosing Plaintiff and Class members' PHI without their written authorization. Defendant violated Cal. Civ. Code § 56, *et seq*., and their legal duty to protect the confidentiality of such information.

59. Defendant also violated Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential PHI. As a direct and proximate result of Defendant's wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members' confidential PHI was viewed, released and disclosed without their authorization by unauthorized persons.

60. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violation of the CMIA, Plaintiff and Class members also are entitled to (1) injunctive relief; (2) punitive damages of up to $3,000 per Plaintiff and each Class member, and; (3) attorneys' fees, litigation expenses and court costs under Cal. Civ. Code § 56.35.

SECOND COUNT

Violation of the California Unfair Competition Law

(Cal Bus. & Prof. Code § 17200, *et seq*.)

(On Behalf of Plaintiff and All Class Members)

51. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

52. The California Unfair Competition Law, Cal Bus. & Prof. Code § 17200, *et seq*., prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

53. In the course of conducting its business, Defendant committed "unlawful business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and Class members' PII/PHI, and violating the statutory and common law alleged herein in the process, including, *inter alia*, the California CMIA, the California CRA, and the California IPA. Plaintiff and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

54. Defendant also violated the UCL by failing to timely notify Plaintiff and Class members regarding the unauthorized release and disclosure of their PII/PHI. If Plaintiff and Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII/PHI, medical information, and identities.

55. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair business

acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends public policy, and is immoral, unethical, oppressive, and unscrupulous. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

56. The UCL also prohibits any "fraudulent business act or practice, above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

57. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiff and Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which he or she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of his or her PII/PHI; (4) statutory damages under the California CMIA; (5) deprivation of the value of his or her PII/PHI, for which there is a well-established national and international market; and/or (v) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

58. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class members, and the general public, also seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to it, as well as all other relief the Court deems appropriate, consistent with Cal. Bus. & Prof. Code § 17203.

THIRD COUNT

Negligence

(On Behalf of Plaintiff and All Class Members)

61. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

62. Plaintiff brings this claim individually and on behalf of the Class members.

63. Defendant knowingly collected, came into possession of, and maintained Plaintiff and Class members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

64. Defendant had, and continues to have, a duty to timely disclose that Plaintiff and Class members' Private Information within its possession was compromised and precisely the type(s) of information that were compromised.

65. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff and Class members' Private Information.

66. Defendant systematically failed to provide adequate security for data in its possession.

67. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff and Class members' Private Information within Defendant's possession.

68. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff and Class members' Private Information.

69. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class members that their Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

70. Defendant's breach of duties owed to Plaintiff and Class members' caused Plaintiff and Class members' Private Information to be compromised.

71. As a result of Defendant's ongoing failure to notify Plaintiff and Class members regarding what type of Private Information has been compromised, Plaintiff and Class members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

72. Defendant's breaches of duty caused Plaintiff and Class members to suffer from identity theft, phishing, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

73. As a result of Defendant's negligence and breach of duties, Plaintiff and Class members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

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

75. In failing to secure Plaintiff and Class members' Private Information and promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiff and Class members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of herself and the Class.

76. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling Defendant to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

FOURTH COUNT

Intrusion Upon Seclusion / Invasion of Privacy

(On Behalf of Plaintiff and All Class Members)

77. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

78. Plaintiff and Class members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

79. Defendant's conduct as alleged above intruded upon Plaintiff and the Class members' seclusion under common law.

80. By failing to keep Plaintiff and Class members' Private Information safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant invaded Plaintiff and Class members' privacy by:

a. Intruding into Plaintiff and Class members' private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about the Plaintiff and Class members, which is highly offensive to a reasonable person.

81. Defendant knew, or acted with reckless disregard of the fact, that a reasonable person in Plaintiff or Class members' position would consider Defendant's actions highly offensive.

82. Defendant invaded Plaintiff and Class members' right to privacy and intruded into Plaintiff and Class members' private affairs by misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

83. As a proximate result of such misuse and disclosures, Plaintiff and Class members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiff and Class members' protected privacy interests.

84. In failing to protect Plaintiff and Class members' Private Information, and in misusing and/or disclosing their Private Information, Defendant has acted with malice and oppression and in conscious disregard of Plaintiff and Class members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages, including punitive damages, on behalf of herself and the Class.

FIFTH COUNT

California Constitutional Right to Privacy

(On Behalf of Plaintiff and All Class Members)

85. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

86. Plaintiff and Class members have reasonable expectations of privacy with regard to their Private Information disclosed to or gathered by a health care provider.

87. The reasonableness of such expectation of privacy is supported by Defendant's unique position as healthcare provider for Plaintiff and Class members, which further requires additional confidentiality and privacy as required by the Health Insurance Portability and Accountability Act.

88. The reasonableness of such expectation of privacy is further supported by Defendant's Notice of Privacy Practices, which, upon information and belief, is provided to patients before any services are rendered.

89. By failing to implement and maintain reasonable security procedures and practices appropriate to protect the Private Information from unauthorized access, destruction, use, modification, or disclosure, Defendant intruded on and into Plaintiff and Class members' solitude, seclusion, or private affairs

90. These intrusions are highly offensive to a reasonable person.

91. Plaintiff and Class members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

92. Defendant's actions, inactions, and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff and Class members.

93. As a result of Defendant's actions, Plaintiff and Class members seek injunctive relief in the form of requiring Defendant to establish appropriate security methods to collect data, to safeguard its information systems, and to secure and safeguard the computerized data of Plaintiff and Class members.

94. As a result of Defendant's actions or inactions, Plaintiff and Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiff and Class members seek punitive damages because Defendants' actions—which were reckless, malicious, oppressive, and willful—were made in conscious disregard of Plaintiffs' rights. Punitive damages are warranted to deter Defendant from engaging in future misconduct.

SIXTH COUNT

California Consumers Legal Remedies Act

(Cal. Civ. Code §§ 1750-1784, *et seq*.)

(On Behalf of Plaintiff and All Class Members)

95. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

96. Defendant is a "person" as defined by Cal. Civ. Code § 1761(c).

97. Defendant's products and services are "goods" and "services" as defined by Cal. Civ. Code § 1761(a) & (b).

98. Defendant advertised, offered, or sold goods or services in California and engaged in trade or commerce directly or indirectly affecting the people of California.

99. Defendant engaged in acts of deception. Other policies, acts, and practices were designed to, and did, induce the use of the products and services for personal purposes by Plaintiff and Class members, and violated and continue to violate the following sections of the CLRA:

a. § 1770(a)(5): Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that he or she does not have;

b. § 1770(a)(7): Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another;

c. § 1770(a)(10): Advertising goods or services with intent not to supply reasonably expectable demand, unless the advertisement discloses a limitation of quantity; and

d. § 1770(a)(16): Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

100. Defendant's wrongful business practices constituted, and continue to constitute, a course of conduct in violation of the CLRA.

101. Pursuant to the provisions of Cal. Civ. Code § 1782(a), Plaintiff provided a letter to Defendant with notice of its alleged violations of the CLRA, demanding that Defendant correct such violations, and providing it with the opportunity to correct its business practices. If Defendant does not thereafter correct its business practices, Plaintiff will amend (or seek leave to amend) the complaint to add claims for monetary relief, including restitution and actual damages, under the Consumers Legal Remedies Act.

102. Pursuant to Cal. Civ. Code § 1780, Plaintiff seeks injunctive relief, their reasonable attorney fees and costs, and any other relief that the Court deems proper.

SEVENTH COUNT

Breach of Express Contract

(On Behalf of Plaintiff and All Class Members)

103. The preceding factual statements and allegations are incorporated by reference.

104. Plaintiff and Class members, upon information and belief, entered into express contracts with Defendant that include Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathers on its own from disclosure.

105. Plaintiff and Class members performed their obligations under the contract when they paid for their health care services.

106. Defendant breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was accessed by unauthorized personnel as part of the Data Breach.

107. As a direct and proximate result of the breach, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

EIGHTH COUNT

Breach of Implied Contract

(On Behalf of Plaintiff and All Class Members)

108. The preceding factual statements and allegations are incorporated by reference.

109. Defendant provided Plaintiff and Class members with an implied contract to protect and keep Defendant's patients' private, nonpublic personal, financial and health information when they gathered the information from each of their patients.

110. Plaintiff and Class members would not have provided their personal, financial or health information to Defendant, but for Defendant's implied promises to safeguard and protect Defendant's patients' private personal, financial, and health information.

111. Plaintiff and Class members performed their obligations under the implied contract when they provided their private personal, financial, and health information as a patient and when they paid for the health care service provided by Defendant.

112. Defendant breached the implied contracts with Plaintiff and Class members by failing to protect and keep private the nonpublic personal, financial, and health information provided to them about Plaintiff and Class members.

113. As a direct and proximate result of Defendant's breach of their implied contracts, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

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

115. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and Class members'

Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

116. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

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

118. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

119. Ordering Defendant to disseminate individualized notice of the Data Breach to all Class members;

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

121. For an award of punitive damages, as allowable by law;

122. For an award of attorneys' fees and costs, including expert witness fees;

123. Pre- and post-judgment interest on any amounts awarded; and

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

Dated: July 2, 2019

Respectfully submitted,

/s/ Danielle L. Perry

Danielle L. Perry (SBN 292120)
Gary E. Mason*
WHITFIELD BRYSON & MASON LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Tel: (202) 429-2290
Fax: (202) 429-2294
dperry@wbmllp.com
gmason@wbmllp.com

Gary M. Klinger*
KOZONIS & KLINGER, LTD.
4849 N. Milwaukee Avenue, Suite 300
Chicago, Illinois 60630
Tel: (312) 283-3814
Fax: (773) 496-8617
gklinger@kozonislaw.com

**Pro hac vice forthcoming*

Attorneys for Plaintiff