

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

PAULA WORTHEY, individually and on behalf of all
others similarly situated,

Plaintiff,

v.

AMERICAN MEDICAL COLLECTION AGENCY,
INC., OPTUM360 SERVICES, INC., QUEST
DIAGNOSTICS INCORPORATED, and DOES 1-10,

Defendants.

Case No. 7:19-cv-5210

CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiff Paula Worthey, on behalf of herself and all others similarly situated, through the undersigned counsel, hereby alleges the following, against Defendants American Medical Collection Agency, Inc. (“AMCA”), Optum360 Services, Inc. (“Optum360”), and Quest Diagnostics Incorporated (“Quest”) (collectively, “Defendants”), upon her own knowledge or, where she lacks personal knowledge, upon information and belief including the investigation of her counsel, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action on behalf of a nationwide class and a California Sub-Class (together, the “Classes”) against Defendants because of their failure to protect the confidential information of millions of patients—including financial information (e.g., credit card numbers and bank account information), medical information, personal information (e.g., Social Security Numbers), and/or other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) (collectively, their “Sensitive Information”). Defendants’ wrongful disclosure has harmed Plaintiff.

II. PARTIES

2. Plaintiff Paula Worthey is an individual residing in Ventura, California, who has been a patient of Quest and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

3. Defendant American Medical Collection Agency, Inc. (“AMCA”) is a New York corporation with its principal place of business in Elmsford, New York.

4. Defendant Quest Diagnostics Incorporated (“Quest”) is a Delaware corporation with its principal place of business in Secaucus, New Jersey.

5. Based on information and belief, Defendant Optum360 Services, Inc. (“Optum360”) is a Delaware corporation with its principal place of business in Eden Prairie Minnesota.

III. JURISDICTION AND VENUE

6. Subject Matter Jurisdiction. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) in that: (1) this is a class action involving more than 1,000 class members; (2) minimal diversity is present as Plaintiff is a citizen of California (and the proposed class members are from various states) while Defendants are citizens of the States of New York, Delaware, and New Jersey; and (3) the amount in controversy exceeds the sum of \$5,000,000, exclusive of interest and costs.

7. Personal Jurisdiction. This Court has personal jurisdiction over Defendants because Defendants do business in and throughout the State of New York, and the wrongful acts alleged in this Complaint were committed in New York, among other venues.

8. Venue. Venue is proper in this District pursuant to: (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiff’s claims occurred in this District, and 28 U.S.C. § 1391(d) because the transactions giving rise to the claims occurred in Westchester County, New York; and (2) 28 U.S.C. § 1391(b)(3) in that Defendants are subject to personal jurisdiction in this District.

IV. FACTUAL ALLEGATIONS

9. Quest is the world’s leading provider of medical diagnostic testing services. It performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease.

10. On June 3, 2019, Quest publicly admitted in a filing with the Securities and Exchange Commission (“SEC”) that: “On May 14, 2019, American Medical Collection Agency (AMCA), a billing collections vendor, notified Quest . . . and Optum360 LLC, [Quest’s] revenue cycle management provider,” of a massive data breach compromising the Sensitive Information of 11.9 million Quest patients, and most likely others (the “Data Breach”). Quest Form 8-K, June 3, 2019.

11. Quest’s SEC filing disclosed that, “between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA’s system that contained information that AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself[,] . . . include[ing] financial information (e.g., credit card numbers and bank account information), medical information[,] and other personal information (e.g., Social Security Numbers).” *Id.*

12. Quest apparently allowed hackers to access Plaintiff’s and other Class Members’ Sensitive Information for some seven months, and did nothing to let the victims know about the Data Breach for nearly a year after it began.

13. Although Quest knew of the Data Breach at least as of May 14, 2019, and although AMCA knew of it even earlier, neither took any steps to notify patients whose information was affected until June 3, 2019, at which point Quest only did so through an SEC filing.

14. Defendants had obligations created by HIPAA, arising from promises made to patients like Plaintiff and other Class Members, and based on industry standards, to keep the compromised Sensitive Information confidential and to protect it from unauthorized disclosures. Class Members provided their Sensitive Information to Quest with the understanding that Quest and any business partners to whom Quest disclosed the Sensitive Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

15. Indeed, Quest promises patients that it will keep their Sensitive Information confidential, assuring patients that it is “committed to protecting the privacy of your identifiable health information.” <<http://questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html>> (last visited June 3, 2019).

16. In its Notice of Privacy Practices, Quest acknowledges that it is subject to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). *Id.*

17. Quest informs patients: “We may provide your PHI [(Private Health Information)] to other companies or individuals that need the information to provide services to us. These other entities, known as ‘business associates,’ are required to maintain the privacy and security of PHI.” *Id.*

18. Defendants’ data security obligations and promises were particularly important given the substantial increase in data breaches — particularly those in the healthcare industry — preceding August 2018, which were widely known to the public and to anyone in Defendants’ industries.

19. Defendants’ security failures demonstrate that they failed to honor their duties and promises by not:

- a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Adequately protecting Plaintiff’s and the Classes’ Sensitive Information;
- c. Ensuring the confidentiality and integrity of electronic protected health information they created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- d. Implementing technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

- e. Implementing policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);
- f. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- g. Protecting against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 C.F.R. § 164.306(a)(2);
- h. Protecting against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);
- i. Ensuring compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or
- j. Training all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

It is Well Established That Data Breaches Lead to Identity Theft

20. Plaintiff and other Class Members have been injured by the disclosure of their Sensitive Information in the Data Breach.

21. The United States Government Accountability Office noted in a June 2007 report on Data Breaches (“GAO Report”) that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in a person’s name.¹ As the GAO Report states, this type of identity theft is the most

¹ See *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government

harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

22. In addition, the GAO Report states that victims of identity theft will face “substantial costs and inconveniences repairing damage to their credit records” and their “good name.”²

23. Identity theft victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such as social security numbers (“SSNs”) for a variety of crimes, including credit card fraud, phone or utilities fraud, and/or bank/finance fraud.

24. There may be a time lag between when Sensitive Information is stolen and when it is used. According to the GAO Report:

“[L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.”³

25. With access to an individual's Sensitive Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name. Identity thieves 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.⁴

Accountability Office, available at <<https://www.gao.gov/new.items/d07737.pdf>> (last visited June 3, 2019).

² *Id.* at 2, 9.

³ *Id.* at 29 (emphasis added).

⁴ See Federal Trade Commission, *Warning Signs of Identity Theft*, available at

26. Sensitive Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Sensitive Information directly on various Internet websites making the information publicly available.

27. A study by Experian found that the “average total cost” of medical identity theft is “about \$20,000” per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.⁵ Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

28. Medical databases are especially valuable identity thieves. According to a 2012 Nationwide Insurance report, “[a] stolen medical identity has a \$50 street value – whereas a stolen social security number, on the other hand, only sells for \$1.”⁶ In fact, the medical industry has experienced disproportionately higher instances of computer theft than any other industry.

V. CLASS ACTION ALLEGATIONS

29. Class Definition. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiff brings this case as a class action on behalf of a Nationwide Class, and a California Sub-Class, defined as follows:

Nationwide Class: All persons in the United States whose Sensitive Information was maintained on the AMCA systems that were compromised as a result of the breach announced by Quest on or around June 3, 2019.

<https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last visited May 28, 2019).

⁵ See Elinor Mills, Study: Medical identity theft is costly for victims, CNET (Mar. 3, 2010), <<https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/>> (last visited June 3, 2019).

⁶ Study: Few Aware of Medical Identity Theft Risk, Claims Journal, <http://www.claimsjournal.com/news/national/2012/06/14/208510.htm> (last visited June 3, 2019).

California Sub-Class: All persons in the State of California whose Sensitive Information was maintained on the AMCA systems that were compromised as a result of the breach announced by Quest on or around June 3, 2019.

Excluded from the above Classes are Defendants, any entity in which Defendants have a controlling interest or that have a controlling interest in Defendants, and Defendants' legal representatives, assignees, and successors. Also excluded are the Judge to whom this case is assigned and any member of the Judge's immediate family.

30. Numerosity. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

31. Commonality. There are numerous questions of law and fact common to Plaintiff and Class Members. These common questions of law and fact include, but are not limited to, the following:

- a. Whether Defendants' data security systems prior to the Data Breach met the requirements of laws including, for instance, HIPAA;
- b. Whether Defendants' data security systems prior to the Data Breach met industry standards;
- c. Whether Plaintiff's and other Class members' Sensitive Information was compromised in the Data Breach; and
- d. Whether Plaintiff's and other Class members are entitled to damages as a result of Defendants' conduct.

32. Typicality. Plaintiff's claims are typical of the claims of the Classes' claims. Plaintiff suffered the same injury as Class Members—*i.e.*, upon information and belief Plaintiff's Sensitive Information was compromised in the Data Breach.

33. Adequacy. Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiff nor her counsel have interests that are contrary to or that conflict with those of the proposed Classes.

34. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and other Class Members. The common issues arising from this conduct that affect Plaintiff and Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

35. Superiority. A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class Members' interests in individually controlling the prosecution of separate actions is low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendants. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Defendants' records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove Plaintiff's claims

as well as the claims of other Class Members. Finally, proceeding as a class action provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

36. Injunctive and Declaratory Relief Appropriate. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants have acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

FIRST CLAIM FOR RELIEF

Negligence

(On behalf of Plaintiff and the Nationwide Class)

37. Plaintiff realleges and incorporates by reference all preceding factual allegations.

38. Quest required Plaintiff and Class Members to submit non-public Personal Information to obtain medical services, which Quest provided to AMCA for billing purposes.

39. By collecting and storing this data, and sharing it and using it for commercial gain, Defendants both had a duty of care to use reasonable means to secure and safeguard this Sensitive Information, to prevent disclosure of the information, and to guard the information from theft.

40. Defendants' duty included a responsibility to implement a process by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

41. Defendants also owed a duty of care to Plaintiff and members of the Classes to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that their systems and networks—and the personnel responsible for them—adequately protected their customers' Sensitive Information.

42. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Quest and its patients, which is recognized by laws including but not limited to HIPAA. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiff and the members of the Classes from a data breach.

43. Defendants' duty to use reasonable security measures also arose under HIPAA, pursuant to which Defendants are required to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

44. In addition, Defendants had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

45. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the common law and the statutes and regulations described above, but also because they are bound by, and have committed to comply with, industry standards for the protection of confidential Sensitive Information.

46. Defendants breached their common law, statutory and other duties—and thus, were negligent—by failing to use reasonable measures to protect patients' Sensitive Information, and by failing to provide timely notice of the Data Breach.

47. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class members' Sensitive Information;

- b. failing to adequately monitor the security of AMCA's networks and systems;
- c. allowing unauthorized access to Plaintiff's and Class members' Sensitive Information;
- d. failing to recognize in a timely manner that Plaintiff's and other Class members' Sensitive Information had been compromised; and
- e. failing to warn Plaintiff and other Class Members about the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

48. It was foreseeable that Defendants' failure to use reasonable measures to protect Sensitive Information and to provide timely notice of the Data Breach would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Classes were reasonably foreseeable.

49. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

50. Accordingly, Plaintiff, on behalf of herself and members of the Classes seek an order declaring that Defendants' conduct constitutes negligence, and awarding damages in an amount to be determined at trial.

SECOND CLAIM FOR RELIEF

Violation of the California Confidential Medical Information Act

(On behalf of Plaintiff and the California Sub-Class)

51. Plaintiff realleges and incorporates by reference all preceding factual allegations.

52. Plaintiff alleges additionally and alternatively that California's Confidential Medical Information Act was enacted to protect, among other things, the release of confidential medical information without proper authorization. *See* Confidential Medical Information Act, Cal. Civ. Code §§ 56, *et seq.* ("CMIA"). To that end, the CMIA prohibits entities from negligently disclosing or releasing any person's confidential medical information. *See* Cal. Civ. Code § 56.36 (2013). The CMIA also requires that an entity that "creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein." Civ. Code § 56.101(a).

53. As described throughout this Complaint, Defendants negligently disclosed and released Plaintiff's and California Sub-Class Members' Sensitive Information by failing to implement adequate security protocols to prevent unauthorized access to Sensitive Information, failing to maintain an adequate electronic security system to prevent data breaches, failing to employ industry standard and commercially viable measures to mitigate the risks of any data breach, and otherwise failing to comply with HIPAA data security requirements.

54. As a direct and proximate result of Defendants' negligence, they disclosed and released Plaintiff's and California Sub-Class Members' Sensitive Information to hackers.

55. Accordingly, Plaintiff seeks to recover actual, nominal (including \$1000 nominal damages per disclosure under Cal. Civ. Code § 56.36(b)), and statutory damages (including under § 56.36(c)) where applicable, together with reasonable attorneys' fees and costs.

THIRD CLAIM FOR RELIEF

Violation of New York General Business Law § 349

(On behalf of Plaintiff and the Nationwide Class)

56. Plaintiff realleges and incorporates by reference all preceding factual allegations.

57. Defendants, while operating in New York, engaged in deceptive acts and practices in the conduct of business, trade and commerce, and the furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a). This includes but is not limited to the following:

a. Defendants failed to enact adequate privacy and security measures to protect the Class Members' Sensitive from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Defendants failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Defendants knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard the Sensitive Information from unauthorized disclosure, release, data breaches, and theft;

d. Defendants omitted, suppressed, and concealed the material fact of Defendants' reliance on, and inadequacy of, AMCA's security protections;

e. Defendants knowingly and fraudulently misrepresented that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Sensitive Information, including but not limited to duties imposed by HIPAA; and

f. Defendants failed to disclose the Data Breach to the victims in a timely and accurate manner, in violation of the duties imposed by, *inter alia*, N.Y. Gen Bus. Law § 899-aa(2).

58. As a direct and proximate result of Defendants' practices, Plaintiff and other Class Members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial and medical accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Sensitive Information.

59. The above unfair and deceptive acts and practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to

Plaintiff and other Class Members that they could not reasonably avoid, which outweighed any benefits to consumers or to competition.

60. Defendants knew or should have known that AMCA's computer systems and data security practices were inadequate to safeguard Sensitive Information entrusted to it, and that risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

61. Plaintiff seeks relief under N.Y. Gen. Bus. Law § 349(h), including but not limited to actual damages (to be proven at trial), treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs. The amount of such damages is to be determined at trial, but will not be less than \$50.00 per violation. *Id.*

62. Plaintiff and Class Members seek to enjoin such unlawful deceptive acts and practices described above. Each Class Member will be irreparably harmed unless the Court enjoins Defendants' unlawful, deceptive actions in that Defendants will continue to fail to protect Sensitive Information entrusted to them, as detailed herein.

63. Plaintiff and Class Members seek declaratory relief, restitution for monies wrongfully obtained, disgorgement of ill-gotten revenues and/or profits, injunctive relief prohibiting Defendant from continuing to disseminate its false and misleading statements, and other relief allowable under N.Y. Gen. Bus. Law § 349.

FOURTH CLAIM FOR RELIEF

Breach of Implied Contract (On Behalf of Plaintiff and the Nationwide Class)

64. Plaintiff incorporates by reference all preceding paragraphs as if fully set forth herein.

65. Plaintiff brings this cause of action on behalf of the Class and to the extent necessary.

66. When Plaintiff and Class members paid money and provided their Sensitive Information to Defendants in exchange for services, they entered into implied contracts with

Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

67. Defendants solicited and invited prospective clients and other consumers to provide their Sensitive Information as part of its regular business practices. These individuals accepted Defendants' offers and provided their Sensitive Information to Defendants. In entering into such implied contracts, Plaintiff and the Class assumed that Defendants' data security practices and policies were reasonable and consistent with industry standards, and that Defendants would use part of the funds received from Plaintiff and the Class to pay for adequate and reasonable data security practices.

68. Plaintiff and the Class would not have provided and entrusted their Sensitive Information to Defendants in the absence of the implied contract between them and Defendants to keep the information secure.

69. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendants.

70. Defendants breached their implied contracts with Plaintiff and the Class by failing to safeguard and protect their Sensitive Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

71. As a direct and proximate result of Defendants' breaches of their implied contracts, Plaintiff and the Class sustained actual losses and damages as described herein.

FIFTH CLAIM FOR RELIEF

Violation of the California Unfair Competition Act, Cal. Bus. & Prof. Code § 17200, *et seq.*

(On behalf of Plaintiff and the California Sub-Class)

72. Plaintiff realleges and incorporates by reference all preceding factual allegations.

73. Defendants' actions as described herein constitute unfair competition within the meaning of the UCL, insofar as the UCL prohibits "any unlawful, unfair or fraudulent business act or practice."

74. Defendants' conducts as alleged herein constitute unlawful, unfair, and fraudulent business practices in that they deceived the Plaintiff and California Sub-Class Members into believing their Sensitive Information would be protected by reasonable, industry-standard data security measures.

75. Defendants' conduct constitutes an "unlawful" business practice within the meaning of the UCL because it violates HIPAA, the California Customer Records Act, Cal. Civ. Code § 17980.80 *et seq.*, and other statutes requiring adequate data security to protect Sensitive Information such as that which was compromised in the Data Breach.

76. Defendants' conduct constitutes an "unfair" business practice within the meaning of the UCL because it is immoral, unethical, oppressive, unscrupulous and/or substantially injurious to consumers.

77. As a direct and proximate result of Defendants' wrongful business practices in violation of the UCL, the California Plaintiff and California Sub-Class Members have suffered injury in fact and lost money or property as a result of purchasing services from Quest. The California Plaintiff and California Sub-Class Members would not have purchased or paid as much for services from Quest had they known the truth about Defendants' data security.

78. Defendants' wrongful business practices constitute a continuing course of conduct of unfair competition since Defendants continues to employ deficient data security.

79. Pursuant to Cal. Bus. & Prof. Code § 17203, the California Plaintiff and the California Sub-Class Members seek an order of this Court enjoining Defendants from continuing to engage in unlawful, unfair, and fraudulent business practices and any other act prohibited by law, including those set forth in this Complaint. The California Plaintiff and the California Sub-Class Members also seek an order requiring Defendants to make full restitution of all moneys it wrongfully obtained from the California Plaintiffs and the Class.

80. Pursuant to Cal. Bus. & Prof. Code § 17203, the California Plaintiff and California Sub-Class Members seek an injunction enjoining Defendant from continuing to employ deficient data security.

SIXTH CLAIM FOR RELIEF

Violation of the California’s Customer Records Act, Cal. Civil Code §§ 1798.81.5 & 1798.82

(On behalf of Plaintiff and the California Sub-Class)

81. Plaintiff realleges and incorporates by reference all preceding factual allegations.

82. “[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.”

83. The Sensitive Information taken in the Data Breach fits within the definition of “Personal information” in Civil Code section 1798.80.

84. Plaintiff and other Class Members provided their personal information to Defendants in order to get medical diagnoses. These patients qualify as “Customer[s]” as defined in Civil Code section 1798.80.

85. By failing to implement reasonable measures to protect the Sensitive Information in their possession, Defendants violated Civil Code section 1798.81.5.

86. In addition, by failing to promptly notify all who were affected by the Data Breach that their Sensitive Information had been acquired (or was reasonably believed to have been acquired) by hackers, Defendants violated Civil Code Section 1798.82.

87. As a direct or proximate result of Defendants’ violations of Civil Code Sections 1798.81, 1798.81.5, and 1798.82, Plaintiff and Class Members were (and continue to be) injured

and have suffered (and will continue to suffer) the damages described in this Class Action Complaint.

88. Defendants' violations of Civil Code Sections 1798.81, 1798.81.5, and 1798.82 were, at a minimum, reckless.

89. In addition, by violating Civil Code Sections 1798.81, 1798.81.5, and 1798.82, Defendants "may be enjoined" under Civil Code Section 1798.84(e).

90. Defendants' violations of Civil Code Section 1798.81.5 and 1798.82 also constitute an unlawful acts or practices under California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 *et seq.*, which affords the Court discretion to enter whatever orders may be necessary to prevent future unlawful acts or practices.

91. Plaintiff accordingly requests that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Defendants utilize strong industry standard encryption algorithms for encryption keys that provide access to stored Sensitive Information; (2) ordering that Defendants implement the use of encryption keys in accordance with industry standards; (3) 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 systems belong to Defendants and all others with whom they share Sensitive Information, on a periodic basis; (4) ordering that Defendants engage third-party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that Defendants audit, test and train their security personnel regarding any new or modified procedures; (6) ordering that Defendants, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendants' computer system is compromised, hackers cannot gain access to other portions of their systems; (7) ordering that Defendants purge, delete, destroy in a reasonable secure manner Sensitive Information no longer

necessary; (8) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (9) 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; and (10) ordering that Defendants implement industry best practices data security systems..

92. Plaintiff further requests that the Court require Defendants to identify and notify all members of the nationwide Class who have not yet been informed of the Data Breach.

93. Plaintiff and the Class are entitled to actual damages in an amount to be determined at trial under Civil Code Section 1798.84.

94. Plaintiff and the Class also are entitled to an award of attorney fees and costs under Civil Code Section 1798.84.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on her own behalf and on behalf of Class Members, pray for judgment against Defendant as follows:

- A. Certification of the proposed Classes;
- B. Appointment of Plaintiff as Class representative;
- C. Appointment of the undersigned counsel as counsel for the Classes;
- D. Declaring that Defendants' actions, as described above, constitute negligence and amounted to violations of HIPAA, the California Customer Records Act, the California Confidential Medical Information Act, and the consumer protection laws of New York, California, and other states;
- H. An award to Plaintiff and the Classes of damages, as allowed by law;
- I. An award to Plaintiff and the Classes of attorneys' fees and costs, as allowed by law and/or equity;
- J. Leave to amend this Complaint to conform to the evidence presented at trial; and

K. Orders granting such other and further relief as the Court deems necessary, just, and proper.

VII. DEMAND FOR JURY

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

Respectfully submitted,

Dated: June 3, 2019

YANKWITT LLP



Russell Yankwitt

russell@yankwitt.com

Michael H. Reed

michael@yankwitt.com

140 Grand Street

Suite 705

White Plains, NY 10601

Tel: 914-686-1500

Fax: 914-487-5000

Tina Wolfson (NY Bar No. 5436043)

twolfson@ahdootwolfson.com

Brad King (NY Bar No. 5588336)

bkink@ahdootwolfson.com

Theodore W. Maya (*pro hac vice* pending)

tmaya@ahdootwolfson.com

AHDOOT & WOLFSON, PC

45 Main Street, Suite 528

Brooklyn, NY 11201

Tel: 917-336-0171

Fax: 917-336-0177

*Counsel for Plaintiff
and the Putative Classes*