Exhibit C12

Duran L. Keller, Esq. (NJ Attorney ID No. 08686-2014)
Of Counsel, The Law Office of Edwyn D. Macelus
PO Box 374
Edgewater, NJ 07020
T: (765) 444-9202
F: (765) 807-3388
Email: duran@kellerlawllp.com

Mark A. Ozzello*
Mark.Ozzello@capstonelawyers.com
Tarek H. Zohdy*
Tarek.Zohdy@capstonelawyers.com
Cody R. Padgett*
Cody.Padgett@capstonelawyers.com
Trisha K. Monesi*
Trisha.Monesi@capstonelawyers.com
Capstone Law APC
1875 Century Park East, Suite 1000
Los Angeles, California 90067
Telephone: (310) 556-4811
Facsimile: (310) 943-0396

**Pro Hac Vice Application Forthcoming*

Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

PATRICK ROGGE and KATHY NEAL, individually, and on behalf of other members of the general public similarly situated,

Plaintiff,

vs.

QUEST DIAGNOSTICS INCORPORATED, LABORATORY CORPORATION OF AMERICA HOLDINGS, BIOREFERENCE LABORATORIES, INC., and OPTUM360, LLC,

Defendants.

Civil Action No.: 2:19-cv-13648

FIRST AMENDED CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Patrick Rogge and Kathy Neal ("Plaintiffs") bring this action against Defendants Quest Diagnostics Incorporated ("Quest"), Laboratory Corporation of America Holdings ("LabCorp"), BioReference Laboratories, Inc., ("BioReference"), (collectively, "the Testing Entities") and Optum360, LLC, (collectively, "Defendants") by and through their attorneys, individually and on behalf of all others similarly situated ("Class Members"), and allege as follows:

JURISDICTION

1. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual Class Members, whose numbers are in excess of 100, exceed the sum value of $5,000,000, exclusive of interests and costs. Plaintiffs are citizens of California, while Defendants are citizens of the States of New York, Delaware, and New Jersey.

2. This Court has personal jurisdiction over Defendants because they have sufficient minimum contacts in New Jersey, or otherwise intentionally avail themselves of the markets within New Jersey to render the exercise for jurisdiction by this Court proper and necessary.

VENUE

3. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District. Defendants have received substantial revenue and profits from their operations in this District. Moreover, venue is proper in this District because Defendant Quest is headquartered in Secaucus, New Jersey.

INTRODUCTION

4. Plaintiffs Patrick Rogge and Kathy Neal, of Roseville, California and Rancho Cordova, California, respectively, bring this action individually and on behalf all Class

Members, *i.e.*, persons in the United States whose Personal Information[1] was stored by Quest, LabCorp, and BioReference, through their agent and vendor, American Medical Collection Agency ("AMCA"), and compromised due to the Subject Data Breach of June 2019.

5. Quest is a massive provider of medical diagnostic testing services. A Fortune 500 company, Quest generated net revenues of $7.7 billion in 2017. Quest's executive offices are located at 500 Plaza Drive, Secaucus, New Jersey 07094. Quest maintains clinical testing laboratories throughout the continental United States, as well as offices, data centers, call centers, distribution centers and patient service centers. In conducting its operations, Quest collects extremely sensitive personal, medical, and financial information from Class Members. Quest contracted with AMCA to house its customers' data.

6. LabCorp is a large provider of medical testing. In conducting its operations, LabCorp collects extremely sensitive personal, medical, and financial information from Class Members. LabCorp contracted with AMCA to house its customers' data.

7. BioReference provides medical test services. In conducting its services, BioReference collects extremely sensitive personal, medical and financial information from Class Members. Like LabCorp and Quest, BioReference contracted with AMCA to house its customers' data. Biorefernece is a subsidiary of OPKO Health, Inc.

8. Optum360 provides revenue services operations. Quest contracts with Optum360, which in turn contracts with AMCA for billing collection services.

9. On June 3, 2019, Quest quietly disclosed—in a Securities and Exchange Commission filing only—that hackers had accessed the Personal Information of 11.9 million of its patients. (the "Subject Data Breach.") The Personal Information, which was stored by Quest's agent, AMCA, included incredibly Personal Information; specifically, HIPAA-protected medical information, bank account information, credit card numbers, and Social Security numbers.

10. Also on June 3, 2019, BioReference disclosed in an SEC filing and press release that

[1] Personal information includes Social Security numbers, financial information (e.g., credit card numbers and bank account information), medical information, other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

hackers had accessed the personal information of its customers housed by BioReference's agent, AMCA. BioReference provided the personal information of 423,000 of its patients to AMCA.

11. On the following day, June 4, 2019, LabCorp disclosed to the media and in an SEC filing that hackers had accessed the personal information of its customers housed by its agent, AMCA. LabCorp provided the personal information of 7.7 million of its patients to AMCA.

12. Quest And Optum 360 knew of the breach by May 14, 2019, if not before, yet Quest waited almost ***three weeks*** to disclose the data breach—and then only disclosed it quietly in an SEC filing. Indeed, Defendants should have known of the Subject Data Breach by March 2019, yet did not attempt to notify their patients until June 3, 2019 (Quest and BioReference) and June 4, 2019 (LabCorp).

13. Per LabCorp's "Notice of Privacy Practices," LabCorp was "required to maintain the privacy of health information that identifies you" and "is committed to the protection of your PHI and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation." LabCorp told its patients that the information shared with its contractors was "for the limited purpose of providing services to us and who are obligated to keep information confidential."

14. Per BioReference's "Notice of Privacy Practices," BioRefenrece was "required by law to protect the privacy of your personal data and PHI." BioRefernece told its patients that its contractors would "take reasonable steps to protect the privacy of your personal data and PHI as required by law and/or contract" and "are directly bound by law and/or contract to protect your information."

15. Defendants knew or should have known that Defendants were failing to protect adequately the Personal Information entrusted to them by their patients, the Class Members. Quests 2018 SEC filing included a section entitled, "**Despite the security measures we have implemented, our IT systems may be subject to unauthorized tampering, cyber attack or other security breach."** In the filing, Quest admitted that "in December 2016, we reported that an internet application on our IT network had been the target of an external cyber attack,

resulting in the theft of certain patient data," that "our IT systems from time to time have experienced other attacks, viruses, attempted intrusions or similar problems" and that "there can be no assurance that we will be able to similarly mitigate future attacks, viruses or intrusions."[2]

16. Because of the data breach, Class Members now face significant risks of identity theft. According to the U.S. Government Accountability Office, perpetuators of fraud can use stolen personal information—such as account numbers, passwords, or Social Security numbers—top take out loans or seek medical care under someone else's name, or make unauthorized purchases on credit cards, among other crimes. Foreign state-based actors can use personal information to support espionage or other nefarious uses.[3]

17. In addition to these hazards, the costs to mitigate the risks from the data breach can be significant to consumers, who will require credit monitoring and/or other services to protect their at-risk identities.

PARTIES and FACTUAL ALLEGATIONS

PLAINTIFFS

Patrick Roggee

18. Plaintiffs Patrick Rogge is a California citizen who resides in Roseville, California.

19. Mr. Rogge is a customer of Defendants and has paid for multiple diagnostic tests performed by Quest.

20. To date, Defendants have not notified Mr. Rogge of the recent data breach.

21. Following Defendants' data breach, Mr. Rogge will have to obtain a copy of his credit report and monitor potentially fraudulent activity.

Kathy Neal

22. Plaintiffs Kathy Neal is a California citizen who resides in Rancho Cordova,

[2] U.S. Securities and Exchange Commission, Form 10-K, Quest Diagnostics Incorporated, *available at* https://www.sec.gov/Archives/edgar/data/1022079/000102207918000038/dgx1231201710-k.htm

[3] U.S. Government Accountability Office, Range of Consumer Risks Highlights Limitations of Identity Theft Services, March 27, 2017, *Available at* https://www.gao.gov/products/GAO-19-230.

California.

23. Ms. Neal is a customer of Defendants and has paid for multiple diagnostic tests performed by Quest, most recently on June 3, 2019.

24. To date, Defendants have not notified Ms. Neal of the recent data breach.

25. On or around April 8, 2019, Ms. Neal suffered credit theft in the amount of approximately $600. As a result, she signed up for LifeLock.

26. Because of Defendants' data breach, Ms. Neal will have to obtain a copy of her credit report and monitor potentially fraudulent activity.

27. Following Defendants' data breach, Ms. Neal will have to obtain a copy of her credit report and monitor potentially fraudulent activity.

DEFENDANTS

28. Defendant Quest Diagnostic Incorporated is a corporation organized and in existence under the laws of the State of Delaware and registered with the New Jersey Department of Corporations to conduct business in New Jersey. It is headquartered in Secaucus, New Jersey.

29. Defendant Laboratory Corporation of America Holdings is a corporation organized and in existence under the laws of the State of Delaware. It is headquartered in Burlington, North Carolina.

30. Defendant BioReference Laboratories, Inc., is a subsidiary of OPKO Health, Inc. It is headquartered in Elmwood Park, New Jersey.

31. Defendant Optum360, LLC is a limited liability company organized and in existence under the laws of the State of Delaware. It is headquartered in Eden Prairie, Minnesota.

FACTUAL ALLEGATIONS

32. Quest is a massive provider of medical diagnostic testing services. A Fortune 500 company, Quest generated net revenues of $7.7 billion in 2017. Quest's executive offices are located at 500 Plaza Drive, Secaucus, New Jersey 07094. Quest maintains clinical testing

laboratories throughout the continental United States, as well as offices, data centers, call centers, distribution centers and patient service centers.

33. LabCorp is a large provider of medical testing. In conducting its operations, LabCorp collects extremely sensitive personal, medical, and financial information from Class Members. LabCorp contracted with AMCA to house its customers' data.

34. BioReference provides medical test services. In conducting its services, BioReference collects extremely sensitive personal, medical and financial information from Class Members. Like LabCorp and Quest, BioReference contracted with AMCA to house its customers' data. Biorefernece is a subsidiary of OPKO Health, Inc.

35. Class Members, who are the patients of Quest, LabCorp, and BioReference, reasonably expected that, in providing their Personal Information, including HIPAA-protected medical information and highly sensitive financial information, Defendants and any vendors to whom quest provided such data would comply with HIPAA and its other duties to keep such data safe from unauthorized disclosure and breach. Indeed, Defendants promised as much in their Notice of Privacy Practices.

36. Specifically, in its Notice of Privacy Practices, Quest acknowledged that it was subject to HIPAA and that Quest was "committed to protecting the privacy of your identifiable health information."[4] Quest specifically stated that its vendors employed adequate measures to keep secure its patients' medical data: "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."

[4] Quest Diagnostics, Notice of Privacy Practices, *available at* https://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html.

37. LabCorp acknowledged in its Notice of Privacy Practices that it was subject to HIPPA, and that it was "required by law to maintain the privacy of health information that identifies you, called protected health information (PHI), and to provide you with notice of our legal duties and privacy practices regarding PHI." LabCorp also represented that it was "committed to the protection of your PHI and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation. We take this commitment seriously and will work with you to comply with your right to receive certain information under HIPAA." Finally, LabCorp represented that "Business Associates - LabCorp may disclose PHI to its business associates to perform certain business functions or provide certain business services to LabCorp. For example, we may use another company to perform billing services on our behalf. All of our business associates are required to maintain the privacy and confidentiality of your PHI. In addition, at the request of your health care providers or health plan, LabCorp may disclose PHI to their business associates for purposes of performing certain business functions or health care services on their behalf. For example, we may disclose PHI to a business associate of Medicare for purposes of medical necessity review and audit."

38. BioReference also acknowledged in its Notice of Privacy Practices that it was subject to HIPPA, and that it was "committed to complying with and addressing data protection requirements under all laws that apply to our business, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA)…." BioReference further stated that it was "We may disclose the minimum amount of your personal data and PHI necessary to contractors, agents and other business associates who need the information to help us with billing or other business activities related to the services we provide. For example, we may share personal data and PHI with a billing company that helps us obtain payment from your insurer, an attorney or with a quality assurance consultant in order to obtain their advice regarding our

operations. If we do disclose your personal data or PHI to a business associate, we will have a written contract with them that requires the business associate and any of its subcontractors to take reasonable steps to protect the privacy of your personal data and PHI as required by law and/or contract. Business associates and their subcontractors are considered to be data processors and, as such, are directly bound by law and/or contract to protect your information…."

39. On June 3, 2019, Quest quietly disclosed—in a Securities and Exchange Commission filing only—that the Personal Information of 11.9 million of its patients had been accessed by criminal hackers. The Personal Information, which was stored by Quest's agent, AMCA, included incredibly Personal Information; specifically, HIPAA-protected medical information, bank account information, credit card numbers, and Social Security numbers.

40. Also on June 3, 2019, BioReference disclosed in an SEC filing and press release that hackers had accessed the personal information of its customers housed by BioReference's agent, AMCA. BioReference provided the personal information of 423,000 of its patients to AMCA.

41. On the following day, June 4, 2019, LabCorp disclosed to the media and in an SEC filing that hackers had accessed the personal information of its customers housed by its agent, AMCA. LabCorp provided the personal information of 7.7 million of its patients to AMCA.

42. In the SEC filing, Quest admitted that "[o]n May 14, 2019, AMCA Collection Agency, a billing collections vendor, notified Quest Diagnostics Incorporated and Optum360 LLC, Quest Diagnostics' revenue cycle management provider, of potential unauthorized activity on AMCA's web payment page."

43. Quest further admitted 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; the information on AMCA's affected system included financial information (e.g., credit card numbers and bank account information), medical information and other personal information (e.g., Social Security Numbers); [and] as of May 31, 2019, AMCA believes that the number of Quest Diagnostics patients whose information was contained on AMCA's affected system was approximately 11.9 million people…."

44. Quest's agent, AMCA, was entrusted with Class Members' Personal Information but failed to take reasonable and adequate measures to protect the Class Members' data from incursion from hostile entities and failed to monitor and detect data breach activity. Because of Quest's negligence, criminal agents had access to the Class Members' Personal Information stored by Quest's agent, AMCA, for a period of eight months.

45. Had Quest, LabCorp, and BioReference taken reasonable and adequate measures to protect Class Members' Personal Information and to monitor its agent's systems adequately, the data breach would not have occurred, or the data breach's duration, reach, and impact would have been greatly diminished.

46. Indeed, Quest, LabCorp, and BioReference failed to monitor properly their vendor, Defendant Optum360, and its sub-vendor, Defendant AMCA, to ensure that their patients' Personal Information was being adequately protected by those entities, including through proper protections against data breach.

47. Moreover, Quest, LabCorp, and BioReference were on notice of the increased risks of data breaches in the health care industry in light of the widely documented increase in health care data breaches in recent years. Furthermore, Quest suffered a data breach in 2016, yet *still* failed to prevent the subject breach.

48. Defendants failed to honor their duties and promises by failing to safeguard adequately Class Members' Personal Information; by failing to maintain an adequate data

security system to lower the data breach and cyber-attack risk; and by failing to train adequately, reasonably, and appropriately all employees and agents to carry out their functions and maintain security of PHI, thus violating 45 C.F.R. § 164.530(b); by reasonably, correctly, and adequately monitoring Defendants' data security systems for intrusions; by ensuring compliance with HIPAA security standard rules by their workforces, thus violating 45 C.F.R. § 164.306(a)(4); by making sure their vendors used adequate and reasonable security measures; by preventing and protecting against reasonably foreseeable and anticipated disclosures or uses of electronic PHI that are unlawful and not allowed under the rules governing privacy of individually identifiable health information, thus violating 45 C.F.R. § 164.306(a)(3); by failing to ensure the integrity and confidentiality of electronic protected health information that Defendants created, received, maintained, and/or transmitted, thus violating 45 C.F.R. § 164.306(a)(1); by failing to protect against reasonably foreseeable and anticipated threats or hazards to the security or integrity of electronic PHI, thus violating 45 C.F.R. § 164.306(a)(2); by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, thus violating 45 C.F.R. § 164.312(a)(1); and/or by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, thus violating 45 C.F.R. § 164.308(a)(1)(i).

49. As a result of the data breach, Plaintiffs and Class Members have suffered damage, as their Personal Information has been compromised. Plaintiffs and Class Members are likely to incur monetary losses due to fraud. For example, Plaintiffs and Class Members are liable to suffer identity theft, including utility or other accounts opened in their name, fraudulent tax returns, medical accounts/services in their name, and loans or credit cards fraudulently taken out in their name. They may also incur monetary damages in efforts to protect themselves against

the above risks, including acquiring credit reports and ordering credit report monitoring or freezes. Moreover, Plaintiffs and Class Members have spent and will continue to spend significant time monitoring their financial and/or medical accounts for misuse. Indeed, because years may elapse between the data of the data breach and the identity theft or other fallout, Plaintiffs and Class Members will be required to continually monitor their credit and/or medical accounts for years.

50. Courts have recognized "loss of value" damages in data breach cases. Plaintiffs and Class Members have suffered such "loss of value" of their stolen Personal Information. Indeed, the Personal Information stolen in the subject data breach is highly valuable and is posted, traded, and sold black market websites. In particular, medical information is highly valuable in this active market, and the health care industry has accordingly been a high frequency target of data breach attacks. Although Defendant knew this and were on notice, they failed to protect Class Members' data adequately.

51. Plaintiffs and Class Members who paid Quest directly further suffered benefit of the bargain damages, given that they overpaid for a service that ostensibly included data security, but in reality, did not. A portion of the price paid was for adequate data security and monitoring. Plaintiffs and Class Members did not get what they bargained for because Quest did not adequately secure or monitor their data.

CLASS ACTION ALLEGATIONS

52. Plaintiffs bring this action individually and on behalf of a nationwide class pursuant to Fed. R. Civ. Pr. P. 23(a), 23(b)(2), and/or 23(b)(3); specifically, the following Class:

The Class: All persons in the United States whose Personal Information was compromised due to the Subject Data Breach disclosed on June 3, 2019.

The California Sub-Class: All persons in the State of California whose Personal Information was compromised due to the Subject Data Breach disclosed on June 3, 2019.

53. Excluded from the Class are: (1) Defendant, any entity or division in which Defendant has a controlling interest, and its legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) those persons who have suffered personal injuries as a result of the facts alleged herein. Plaintiffs reserve the right to amend the Class definition and/or add Sub-Classes if discovery and further investigation reveal that the Class should be expanded or otherwise modified.

54. There is a well-defined community of interest in the litigation and the Class is readily ascertainable.

55. Numerosity: Although the exact number of Class Members is uncertain and can only be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable. The disposition of the claims of these Class Members in a single action will provide substantial benefits to all parties and to the Court. The Class Members are readily identifiable from information and records in Defendants' possession, custody or control.

56. Typicality: The claims of representative Plaintiffs are typical of the claims of the Class in that the representative Plaintiffs, like all Class Members, were on information and belief subject to the compromise of their Personal Information in the subject data breach.

57. Commonality: There are numerous questions of law and fact common to Plaintiffs and the Class that predominate over any question affecting only individual Class Members. These common legal and factual issues include the following:

a. Whether Plaintiffs and Class Members suffered legally cognizable damages because of Defendants' misconduct;

b. Whether Defendants complied with applicable data security laws and regulations; for example, HIPAA;

c. Whether Defendants' systems for data security before and during the subject data breach were on par with the standards in the industry;

d. Whether Plaintiffs and Class Members are entitled to injunctive relief;

e. Whether Defendants owed a duty to protect Class Members' Personal

Information;

f. Whether Defendants knew or should have known that their systems for monitoring and protecting data were insufficient;

g. Whether Defendants breached their duty to Class Members to protect their Personal Information; and

h. Whether hackers compromised and/or obtained Class Members' Personal Information in the subject data breach.

58. Adequate Representation: Plaintiffs will fairly and adequately protect the interests of the Class Members. Plaintiffs have retained attorneys experienced in the prosecution of class actions, including consumer and product defect class actions, and Plaintiffs intend to prosecute this action vigorously.

59. Superiority: Plaintiffs and the Class Members have all suffered and will continue to suffer harm and damages as a result of Defendants' unlawful and wrongful conduct. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Absent a class action, most Class Members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Because of the relatively small size of the individual Class Members' claims, it is likely that only a few Class Members could afford to seek legal redress for Defendants' misconduct. Absent a class action, Class Members will continue to incur damages, and Defendants' misconduct will continue without remedy. Class treatment of common questions of law and fact would also be a superior method to multiple individual actions or piecemeal litigation in that class treatment will conserve the resources of the courts and the litigants and will promote consistency and efficiency of adjudication.

60. In the alternative, the Class may be certified because:

a. the prosecution of separate actions by the individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual Class Members, which would establish incompatible standards

of conduct for Defendants;

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

c. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final and injunctive relief with respect to the members of the Class as a whole.

VIOLATIONS ALLEGED

COUNT I

NEGLIGENCE

(On Behalf of the Class and California Sub-Class)

61. Plaintiffs and Class Members incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

62. Quest, LabCorp, and BioReference required Plaintiffs and Class Members to submit non-public personal information in order to obtain medical services, which it forwarded to Optum360 and/or AMCA for billing purposes.

63. By collecting and storing this data, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard Class Members' Personal Information, to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes 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.

64. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to

ensure that their systems and networks, and the personnel responsible for them, adequately protected the Personal Information.

65. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Quest, LabCorp, and BioReference and their client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

66. Defendants' duty to use reasonable security measures under HIPAA required Defendants 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). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

67. In addition, Defendants had a duty to employ 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.

68. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Personal Information.

69. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Personal Information, and by failing to provide timely notice of the Data Breach. 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 Class Members' Personal Information;

b. Failing to adequately monitor the security of AMCA's networks and

systems;

c. Failure by Quest, LabCorp, and BioReference to periodically ensure that their vendors, including Optum360 and AMCA, had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Personal Information;

e. Failing to detect in a timely manner that Class Members' Personal Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

70. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Personal Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of data breaches in the medical industry.

71. It was therefore foreseeable that the failure to adequately safeguard Class Members' Personal Information would result in one or more types of injuries to Class Members.

72. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

73. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, e.g.,: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all Class Members.

COUNT II

BREACH OF IMPLIED CONTRACT

(On Behalf of the Class and the California Sub-Class)

74. Plaintiffs and Class Members incorporate by reference each preceding and

succeeding paragraph as though fully set forth at length herein.

75. Plaintiffs re-alleges and incorporates by reference all preceding allegations.

76. When Plaintiffs and Class Members provided their Personal Information to Defendants in exchange for Defendants' services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

77. Defendants solicited and invited Class Members to provide their Personal Information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their Personal Information to Defendants.

78. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

79. Class Members were aware of, or reasonably anticipated that, Quest, LabCorp, and BioReference would forward certain Personal Information to vendors, as disclosed in Quest, LabCorp, and BioReference's Notices of Privacy Practices.

80. Class Members who paid money to Quest, LabCorp, and BioReference reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

81. Plaintiffs and Class Members would not have entrusted their Personal Information to Defendants in the absence of the implied contract between them and Defendants to keep the information reasonably secure. Plaintiffs and Class Members would not have entrusted their Personal Information to Quest, LabCorp, and BioReference in the absence of Quest, LabCorp, and BioReference's implied promise to monitor their vendors to ensure that they adopted reasonable data security measures.

82. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

83. Defendants breached their implied contracts Class Members by failing to safeguard and protect their Personal Information. Quest, LabCorp, and BioReference breached their

implied contract with Class Members by failing to properly monitor the data security practices of their vendors, Defendants Optum360 and AMCA.

84. As a direct and proximate result of Defendants' breaches of the implied contracts, Class Members sustained damages as alleged herein.

85. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

86. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, e.g.,: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all Class Members.

COUNT III

(Violation of California Business and Professions Code § 17200, et seq.)

(On Behalf of the Class, or, in the alternative, the California Sub-Class)

87. Plaintiffs and Class Members incorporate by reference each proceeding and succeeding paragraph as though fully set forth at length herein.

88. Plaintiffs bring this cause of action on behalf of themselves and on behalf of the Nationwide Class, or in the alternative, on behalf of the California Sub-Class.

89. As a result of their reliance on Defendants' representations and omissions, Class Members suffered an ascertainable loss due to Defendants' failure to provide adequate protection of Class Members' personal and confidential information. This loss was also the direct result of Defendants' failure to provide timely and sufficiently informative notice and warning of potential and actual cybersecurity breaches.

90. California Business & Professions Code § 17200 prohibits acts of "unfair competition," including any "unlawful, unfair or fraudulent business act or practice" and "unfair, deceptive, untrue or misleading advertising."

91. Plaintiffs and Class Members are reasonable consumers who expected Defendant to protect vigorously the personal information entrusted to Defendants and to be informed by

Defendants of potential and actual cybersecurity vulnerabilities as soon as Defendants became aware of such threats.

92. Defendants' acts and omissions were intended to induce Plaintiffs and Class Members' reliance on Defendants' promise that their personal information was secure and protected and/or their failure to disclose otherwise, to increase the number of Class Members, and, ultimately, to increase Defendants' revenues. Plaintiffs and the Class Members were deceived by Defendants' failure to properly implement adequate, commercially reasonable security measures to protect their personal information, and Defendants' failure to promptly notify them of the security breach. As a result, Defendants' conduct constitutes "fraudulent" business acts or practices.

93. Defendants' conduct was and is likely to deceive consumers.

94. In failing to implement adequate security procedures and protocols to protect Plaintiffs' and Class Members' Personal Information, and to promptly notify Plaintiffs and Class Members of potential and actual security threats, Defendants have knowingly and intentionally concealed material facts and breached their duty not to do so.

95. Defendants were under a duty to Plaintiffs and Class Members to protect Class Members' Personal Information and promptly notify Class Members of potential and actual security threats, and other omitted facts alleged herein, because:

- Defendants were in a superior position to know the specifics of a potential or actual security breach; and
- Defendants actively concealed information known to them regarding potential and actual security breaches affecting Class Members' account information.

96. The facts Defendant concealed from or did not disclose to Plaintiffs and Class Members are material in that a reasonable person would have considered them to be important in deciding whether to use Defendants' services. Had Plaintiffs and other Class Members known that Defendants failed to employ necessary and adequate protection of their Personal Information and would fail to timely notify them of potential security breaches, they would not

have used Defendants' services.

97. By their conduct, Defendants have engaged in unfair competition and unlawful, unfair and fraudulent business practices. Defendants' unfair or deceptive acts or practices occurred repeatedly in Defendants' trade or business and were capable of deceiving a substantial portion of the purchasing public. 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. 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 Personal Information such as that which was compromised in the subject data breach.

98. As a direct and proximate result of Defendants' unlawful, unfair and deceptive practices, Plaintiffs and Class Members suffered and will continue to suffer injury in fact. Plaintiffs and Class Members lost money or property as a result of purchasing services from Defendants.

99. Defendants have been unjustly enriched and should be required to make restitution to Plaintiffs and Class Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs 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.

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

COUNT IV

(Violation of the California Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.*)

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

101. Plaintiffs and the California Sub-Class incorporate by reference each proceeding and succeeding paragraph as though fully set forth at length herein.

102. The California Legislature enacted Civil Code § 1798.81.5 "to ensure that personal information about California residents is protected." The statute requires that any business that "owns, licenses, or maintains personal information about a California resident … 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."

103. Defendants are "businesses" as defined by Cal. Civil Code § 1798.80(a).

104. Plaintiffs and California Sub-Class Members are "individual[s]" as defined by Cal. Civil Code § 1798.80(d).

105. The personal information taken in the data breach was "personal information" as defined by Cal. Civil Code § 1798.80(e) and 1798.81.5(d), which includes:

> "information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information."

106. The breach of the Personal Information of Class Members users was a "breach of the security system" of Defendant as defined by Cal. Civil Code § 1798.82(g).

107. By failing to implement reasonable security measures which would appropriately secure the personal information of Class Members, Defendants violated Cal. Civil Code § 1798.81.5.

108. In addition, by failing to immediately notify all affected Class Members that their Personal Information had been acquired or may have been acquired by unauthorized persons in

the data breach, Defendants violated Cal. Civil Code § 1798.82. Defendants' failure to immediately notify Class Members of the breach caused Class Members to suffer damages because they have lost the opportunity to immediately:

a) buy identity protection, monitoring, and recovery services;

b) flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service;

c) purchase or otherwise obtain credit reports; monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or medical services;

d) place and renew credit fraud alerts on a quarterly basis;

e) routinely monitor public records, loan data, or criminal records;

f) contest fraudulent charges and other forms of criminal, financial and medical identity theft, and repair damage to credit and other financial accounts;

g) and, take other steps to protect themselves and recover from identity theft and fraud.

109. Because they violated Cal. Civil Code § 1798.81.5 and 1798.82, Defendants "may be enjoined" under Cal. Civil Code § 1798.84(e).

110. Plaintiffs request that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures to protect Class Members' personal information, including, but not limited to, ordering that Defendants:

a) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

b) engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices;

c) audit, test, and train its security personnel regarding any new or modified

procedures;

d) conduct regular database scanning and securing checks consistent with prudent industry practices;

e) 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 consistent with prudent industry practices;

f) receive periodic compliance audits by a third party regarding the security of the computer systems, cloud-based services, and application software Defendants use to store the personal information of Class Members;

g) meaningfully educate Class Members 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

i) provide ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and Class Members.

111. As a result of Defendants' violation of Cal. Civ. Code § 1798.81.5, Plaintiffs and Class Members have incurred and will incur damages, including but not necessarily limited to:

a) the loss of the opportunity to control how their Personal Information is used;

b) the diminution in the value and/or use of their personal information entrusted to Defendants for the purpose of deriving services from Defendants and with the understanding that Defendants would safeguard their Personal Information against theft and not allow access and misuse of their personal information by others;

c) the compromise, publication, and/or theft of their Personal Information; out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts;

d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and

recover from identity data misuse;

e) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets;

f) unauthorized use of compromised personal information to open new financial and/or health care or medical accounts; tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected;

g) the continued risk to their Personal Information, which remain in Defendants' possession and are subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information in their possession; and

h) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the personal information compromised as a result of the subject data breach for the remainder of the lives of the Class Members.

112. Plaintiffs seek all remedies available under Cal. Civil Code § 1798.84, including actual and statutory damages, equitable relief, and reasonable attorneys' fees. Plaintiffs also seeks reasonable attorneys' fees and costs under applicable law including California Code of Civil Procedure § 1021.5.

COUNT V

(Deceit by Concealment, Cal. Civ. Code §§ 1709, 1710)

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

113. Plaintiffs and the Classes incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

114. Defendants had an obligation to disclose to all Class Members that their Personal Information was an easy target for hackers and Defendants were not implementing measures to protect them.

115. Defendants did not do these things. Instead, Defendants willfully deceived Plaintiffs

and the Class Members by concealing the true facts concerning their data security, which Defendants were obligated and had a duty to disclose. Additionally, Defendants represented to users in effect that their Personal Information and other data was safe and that Defendants were dedicated to maintaining that security.

116. Had Defendants disclosed the true facts about their poor data security, Plaintiffs and the Class Members would have taken measures to protect themselves. Plaintiffs and the Class Members justifiably relied on Defendants to provide accurate and complete information about Defendants' data security, and Defendants did not. Further, independent of any representations made by Defendants, Plaintiffs and the Class justifiably relied on Defendants to provide a service with at least minimally adequate security measures and justifiably relied on Defendants to disclose facts undermining that reliance.

117. Rather than cease offering a clearly unsafe and defective services or disclosing to Plaintiffs and the Class Members that its services were unsafe and users' Personal Information was exposed to theft on a grand scale, Defendants continued and concealed information relating to the inadequacy of their security.

118. These actions are "deceit" under Cal. Civil Code § 1710 in that they are the suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.

119. As a result of this deceit by Defendants, they are liable under Cal. Civil Code § 1709 for "any damage which [Plaintiffs and the Class] thereby suffer[]."

120. As a result of this deceit by Defendants, the Personal Information of Plaintiffs and the Members Class was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Personal Information was disclosed to third parties without their consent. Plaintiffs and Class Members also suffered diminution in value of their Personal Information in that it is now easily available to hackers on the Dark Web. Plaintiffs and/or the Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and/or other expenses relating to identity theft

losses or protective measures.

121. Defendants' deceit as alleged herein is fraud under Civil Code § 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants conducted with the intent on the part of Defendants of depriving Plaintiffs and the Class of "legal rights or otherwise causing injury." As a result, Plaintiffs and the Class Members are entitled to punitive damages against Defendants under Cal. Civil Code § 3294(a).

COUNT VI

(Breach of Confidence)

(On behalf of Plaintiffs and on behalf of the Class and California Sub-Class)

122. Plaintiffs and Class Members incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

123. This claim is asserted against Defendants for breach of confidence concerning the Personal Information that Plaintiffs and the other Class Members provided to Defendants in confidence.

124. At all times during Plaintiffs' and Class Members' interactions with Defendants, Defendants were fully aware of the confidential nature of the Personal Information that Plaintiffs and Class Members shared with Defendants.

125. Plaintiffs and Class Members reasonably expected that their Personal Information would be collected, stored, and protected in confidence by Defendants, and not disclosed to unauthorized third parties. Plaintiffs and Class Members provided their respective Personal Information to Defendants with the understanding that Defendants would protect and not permit that Personal Information to be disseminated to any unauthorized third parties.

126. Defendants voluntarily received in confidence Plaintiffs' and Class Members'

Personal Information with the understanding that that Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

127. Due to Defendants' failure to prevent, detect, and stop the subject data breach from occurring, Plaintiffs' and Class Members' Personal Information was disclosed and misappropriated to unauthorized malicious third parties beyond their confidence and without their express permission.

128. As a direct and proximate cause of Defendants' actions and inactions, Plaintiffs and Class Members have suffered damages.

129. But for Defendants' disclosure of Personal Information in violation of the parties' understanding that it would be held in confidence, Plaintiffs' and Class Members' Personal Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' disclosure was a direct and legal cause of the theft of Plaintiffs' and Class Members' Personal Information, as well as their resulting damages.

130. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and Class Members' Personal Information. On information and belief, Defendants knew their computer systems and technologies for accepting and securing Plaintiffs' and Class Members' Personal Information had numerous security vulnerabilities, but Defendants continued to collect, store, and maintain Plaintiffs' and Class Members' Personal Information without fixing the vulnerabilities.

131. As a result of Defendants' misconduct, Plaintiffs' and Class Members' Personal Information was compromised – placing them at a greater risk of identity theft and subjecting them to identity theft and fraud – and disclosed to unauthorized, malicious, third parties without their consent. Plaintiffs and Class Members also suffered diminution in value of their Personal Information in that it became easily available to hackers on the dark web. Plaintiffs and Class Members have also suffered consequential out-of-pocket losses for procuring credit freezes or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of members of the Class, respectfully request that this Court:

a. Enter an order certifying this matter as a class action with Plaintiffs as representative of the Plaintiffs Class, and designating Plaintiffs' counsel as Plaintiffs Class counsel;

b. Award all actual, general, special, incidental, statutory, treble, punitive, and consequential damages and counsel fees to which Plaintiffs and Class Members are entitled;

c. Award pre-judgment and post-judgment interest on such monetary relief;

d. Award injunctive relief is appropriate and necessary to remedy Defendants' wrongful conduct and to prevent the wrongful conduct from continuing; and

e. Adjudging and decreeing that the acts alleged herein constitute negligence and amount to violations of HIPAA, the California Customer Records Act, the California Confidential Medical Information Act, the California Unfair Competition Act, and the consumer protection laws of California, and other states;

f. The costs of this suit, including reasonable attorneys' fees; and

g. Award all other relief deemed appropriate by the Court.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demands a trial by jury pursuant to Fed. R. Civ. P. 38 on all claims and issues so triable.

Dated: June 24, 2019

By: /s/ Duran L. Keller

Duran L. Keller, Esq.
Of Counsel, The Law Office of Edwyn D. Macelus
PO Box 374
Edgewater, NJ 07020
T: (765) 444-9202
F: (765) 807-3388
Email: duran@kellerlawllp.com

Mark A. Ozzello*
Mark.Ozzello@capstonelawyers.com
Tarek H. Zohdy*
Tarek.Zohdy@capstonelawyers.com
Cody R. Padgett*
Cody.Padgett@capstonelawyers.com
Trisha K. Monesi*
Trisha.Monesi@capstonelawyers.com
Capstone Law APC
1875 Century Park East, Suite 1000
Los Angeles, California 90067
Telephone: (310) 556-4811
Facsimile: (310) 943-0396

**Pro Hac Vice Application Forthcoming*

LOCAL CIVIL RULE 11.2 CERTIFICATION

I hereby certify that to the best of my knowledge the matter in controversy is the subject of other actions pending before this and other courts, including, among other actions, *Mayer v. Quest Diagnostics, Inc., et al. 5:19-cv-01029; Marler v. Quest Diagnostics, Inc., et al., 8:19-cv-01091; Fernandez v. Quest Diagnostics, Inc., et al., 2:19-cv-13398; Grauberger v. Quest Diagnostics, Inc., et al., 3:19-cv-03102; Gutierrez v. Quest Diagnostics, Inc., et al., 7:19-cv-05212; Lanouette v. Quest Diagnostics, Inc., et al., 7:19-cv-05216; Vieyra v. Quest Diagnostics, Inc., et al., 2:19-cv-13396; Worthey v. Quest Diagnostics, Inc., et al., 7:19-cv-05210; Julin v. Quest Diagnostics, Inc., et al., 2:19-cv-13446; Oswald v. Quest Diagnostics, Inc., et al., 7:19-cv-05302; Carbonneau v. Quest Diagnostics, Inc., et al., 2:19-cv-13472; Meisel v. Quest Diagnostics, Inc., et al., 2:19-cv-13484;* and *Rahill v. Quest Diagnostics, Inc., et al., 2:19-cv-13510.*

I hereby certify that the foregoing statements made by me are true. I am aware that if any of the foregoing statements made by me is willfully false, I am subject to punishment.

Dated: June 24, 2019

Of Counsel, The Law Office of Edwyn D. Macelus

Attorneys for Plaintiffs

/s/ Duran L. Keller
Duran L. Keller, Esq.