James E. Cecchi
CARELLA BYRNE CECCHI
OLSTEIN BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
Tel.: (973) 994-1700
Email: jcecchi@carellabyrne.com

Attorneys for Plaintiff
(Additional Counsel on the Signature Page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

JULIO ANTONIO PEREZ VIEYRA, *individually, and on behalf of all others similarly situated*, *Plaintiff*, v. QUEST DIAGNOSTICS INC.; AMERICAN MEDICAL COLLECTION AGENCY; and Optum360 LLC, *Defendants*.	CASE NO: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Julio Antonio Perez Vieyra, individually on behalf of a class of all that similarly situated (the "Class"), complains against Defendants, and alleges on information and belief as follows:

PRELIMINARY STATEMENT

1. On June 3, 2019, Quest Diagnostics Inc. ("Quest") revealed in a press release and securities filing that an unauthorized user had access and did access the system run by Quest's billing collections vendor, American Medical Collection Agency ("AMCA"), for over

six months between late 2018 and March 2019. Defendants could have prevented this theft had it employed reasonable, industry-standard security measures.

2. Plaintiff brings this class action because Defendants failed to secure and safeguard his medical information, personally identifiable information ("PII")—such as Plaintiff's and Class Members' mailing address, phone number, email address, date of birth, gender, and other personal information—and their credit and debit card numbers and other payment card data ("PCD").

3. Quest admitted to its customers that the information on AMCA's affected system included its customers' financial information—credit card numbers, bank account information (to name two examples)—medical information, and other personal information.

4. As of May 31, 2019, AMCA believed that 11.9 million Quest patients had their information on the affected systems. As of this filing, Quest could not verify the accuracy of this information.

5. Quest collects its customers' private medical and financial information as part of providing blood testing. Quest contracts with Optum360, LLC ("Optum360"). In turn, Optum360 goes to AMCA for billing collection services. Throughout this process, Defendants obtain and share Quest customers' personal information and are charged with safeguarding private medical, personal, and financial information. They failed.

6. Defendants' failure to protect their information is a breach of their contracts with Plaintiff and Class Members and violates their legal duties and state consumer protection and privacy laws.

7. This widespread failure to safeguard its customers' information was directly contrary to Quest's representations in its privacy policy that any information shared to

contractors was "for the limited purpose of providing services to us and who are obligated to keep the information confidential."[1] Quest's "Notice of Privacy Practices" explicitly states that it is "required by law to maintain the privacy of your PHI [protected health information]."[2]

8. Defendants' intentional, willful, reckless, and/or negligent conduct—failing to prevent the breach, failing to limit its severity, and failing to detect it in a timely fashion—damaged Plaintiff and all of the Class Members uniformly. For this reason, Defendants should pay for appropriate identity theft protection and reimburse its customers the money they would not have paid Quest had it disclosed its substandard security practices. Plaintiff's personal information remains stored in Defendants' computer systems. Plaintiff and Class Members are therefore entitled to injunctive and other equitable relief that safeguards their information, requires Defendants to significantly improve their security, and provides independent, expert oversight of Defendants' security systems.

PARTIES

Plaintiff Julio Antonio Perez Vieyra

9. Plaintiff Julio Antonio Perez Vieyra is a citizen and resident of California.

10. Mr. Perez Vieyra went to a Quest laboratory to obtain blood testing in or around 2012.

11. Mr. Perez Vieyra provided Quest with confidential personal information and medical information as part of obtaining blood testing.

[1] Online Privacy Policy, https://www.questdiagnostics.com/home/privacy-policy/online-privacy.html (last visited June 3, 2019).
[2] Notice of Privacy Policies, https://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html, (last visited June 4, 2019).

12. Mr. Perez Vieyra's bill from Quest was subsequently sent to a collections agency by Quest.

13. Upon information and belief, Mr. Perez Vieyra has been contacted through several letters over the subsequent years, including as recently as last month, by AMCA.

14. Mr. Perez Vieyra believed that Quest would protect his confidential information when he provided it to Quest.

15. Mr. Perez Vieyra would not have provided Quest with this confidential information nor used Quest to provide blood testing had he known that it would expose his confidential information.

16. Mr. Perez Vieyra suffered damages due to the data breach.

Defendant Quest Diagnostics Incorporated

17. Quest Diagnostics Incorporated is a Delaware corporation with its principal place of business in Secaucus, New Jersey.

Defendant American Medical Collection Agency

18. American Medical Collection Agency is a New York corporation with its principle place of business in Elmsford, New York.

Defendant Optum360 LLC

19. Optum360, LLC is a Delaware corporation with its principal place of business in Eden Prairie, Minnesota.

JURISDICTION AND VENUE

20. Subject matter jurisdiction is proper because this case has been brought as a class action, the aggregate claims of the Class exceeds $5 million exclusive of interest and costs, the Class includes more than 100 members, and one or more of the members of the

Class resides in a state that is different from the state in which Defendants reside. *See* 28 U.S.C. § 1332(d)(2)(A & C).

21. Personal jurisdiction is proper over Quest because it resides in this district and regularly conducts business here.

22. Personal jurisdiction is proper over AMCA because it regularly conducts business in this district. Upon information and belief, a substantial portion of the events and conduct giving rise to this litigation occurred in this district.

23. Personal jurisdiction is proper over Optum360 because it regularly conducts business in this district. Upon information and belief, a substantial portion of the events and conduct giving rise to this litigation occurred in this district.

24. Venue is proper because Quest is located in and transacts business in this district, a substantial portion of the events and conduct giving rise to the litigation violations complained of in this action occurred in this district, and a substantial portion of the injury from Quest's conduct occurred in this district. Because Quest's headquarters are in this District, efficiencies can be gained by litigating this case here, as documents and evidence—including individuals who may be able to provide deposition testimony—are located within this District. *See* 28 U.S.C. §1391(b)(1&2).

25. Venue is also proper because, upon information and belief, AMCA and Optum360 were involved in the events and conduct giving rise to the litigation that occurred in this District.

ADDITIONAL FACTUAL ALLEGATIONS

A. Quest Collects customers' PII, PCD, and confidential medical information and shares it with Optum360 and AMCA.

26. Quest operates over 2,200 "Patient Service Centers" which are used to draw

and test customers' blood following an order from a doctor.[3]

27. Quest asks its customers to bring photo identification, current health insurance information, and provides methods for payment whether a customer does or does not have insurance that will cover the procedure.[4] Critically, Quest also "obtains diagnostics information from the ordering physicians [sic] office."[5]

28. Quest's invoices cover laboratory testing fees only and are separate from any bill received by a patient's physician. Patients can be charged by either directly going to a Quest Patient Service Center or if their physician has sent their specimen to a Quest Diagnostics laboratory.[6]

29. When certain Quest customers do not pay their invoices within the requested time period, Quest will reach out to its contractor, Optum360 who is then responsible for sending the outstanding balance to a collection agency like AMCA.[7] In September 2016, Optum360 and Quest partnered so that Quest's revenue services operations would become part of Optum360.[8]

---

[3] https://questdiagnostics.com/home/patients/preparing-for-test/get-started (last visited June 3, 2019).
[4] *Id.*
[5] Quest Diagnostics, Frequently Asked Questions: Billing Services, "Where does Quest Diagnostics obtain the diagnosis information related to my claim?" https://billing.questdiagnostics.com/PatientBilling/PATFaqExternal.action?getLabCode=false&fromLink=doFaq (last visited June 3, 2019).
[6] Quest Diagnostics, Frequently Asked Questions: Billing Services, "Why have I received an invoice from Quest Diagnostics?" https://billing.questdiagnostics.com/PatientBilling/PATFaqExternal.action?getLabCode=false&fromLink=doFaq (last visited June 3, 2019).
[7] Quest Diagnostics Incorporated, 2018 Annual Report (Form 10-K), at 58.
[8] Optum and Quest Diagnostics Partner to Help Make the Health System Work Better for Patients, Physicians, Health Plans and Employers, Sept. 13, 2016, https://www.optum.com/about/news/optum-quest-diagnostics-partner-help-make-health-system-work-better-for-patients-physicians-health-plans-employers.html (last visited June 3, 2019).

30. Upon information and belief, in order to facilitate the collection process Optum360 would provide AMCA with Quest customers' confidential medical information, PII, and PCD which AMCA subsequently housed in its own system.

B. Defendants failed to protect Quest customers' documents.

31. On May 14, 2019, AMCA informed Quest and Optum360 of "potential unauthorized activity on AMCA's web payment page."[9]

32. Quest and Optum360 have stated that they "promptly sought information from AMCA about the incident, including what, if any, information was subject to unauthorized access."[10]

33. Prior to AMCA informing Quest and Optum360, the security firm Gemini Advisory notified the website Databreaches.net that their research had found the payment card details of 200,000 patients from AMCA for sale on the dark web. These cards appeared to have been compromised between September 2018 and March 2019—in line with Quest's information.[11]

34. Incredibly, the same article reported that AMCA did not respond to Gemini Advisory and Gemini instead informed law enforcement. Law enforcement then contacted AMCA.[12]

35. While Defendants do not yet know the full extent of the data breach, Quest's securities filing indicated that it AMCA told it that:

> [B]etween 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

[9] Quest Diagnostics Incorporated, Current Report, Form 8-K (June 3, 2019).
[10] *Id.*
[11] Jessica Davis, 11.9M Quest Diagnostics Patients Impacted by AMCA Data Breach, HealthIT Security, June 3, 2019, https://healthitsecurity.com/news/11.9m-quest-diagnostics-patients-impacted-by-amca-data-breach (last visited June 4, 2019).
[12] *Id.*

> entities, including Quest Diagnostics, and information that AMCA collected itself; the information on AMCA's affected system including financial information (*e.g.*, credit card numbers and bank account information), medical information and other personal information (*e.g.*, Social Security Numbers); 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.[13]

36. In response to this news, an AMCA spokesperson stated that "upon receiving information from a security compliance firm that works with credit card companies of a possible security compromise, we conducted an internal review, and then took down our web payments page."[14]

37. Quest, in response, has suspended, but not cancelled, sending collection requests to AMCA, provided notifications to affected health plans, will notify regulators and others as required by federal and state law, and has been working with Defendants and "outside security experts" to investigate the issue and the potential impact.[15]

C. Quest Committed to Safeguarding Its Customers' Personal Information.

38. Quest's contracts with its customers as well as its website commit it to protecting customer information, including when that information is shared with third parties.

39. Quest's website also makes it clear that it will protect payment information. As an initial matter, Quest affirmatively states "yes" in response to the question "Is my payment information secure" on its facts and questions page.[16] It explains that Quest uses "Transport Security Layer (TSL) to encrypt your credit card number, name, and address information so only QuestDiagnostics.com is able to decode your information."[17]

---

[13] *Id.*
[14] Zach Whittaker, "Quest Diagnostics says 11.9 million patients affected by data breach," TechCrunch, June 3, 2019, https://techcrunch.com/2019/06/03/quest-diagnostics-breach/.
[15] Quest Diagnostics Incorporated, Current Report, Form 8-K (June 3, 2019).
[16] Quest Diagnostics, https://myquest.questdiagnostics.com/myquest-faq1/QuestDirect.htm (last visited June 3, 2019).
[17] *Id.*

40. Quest's privacy policy also suggests that "our contractors to who we may provide such information for the limited purpose of providing services to us ***and who are obligated to keep the information confidential***."[18]

41. Quest's privacy policy also offers assurances that "we limit Quest Diagnostics' employees and contractors' access to personal information. Only those employees and contractors with a business reason to know have access to this information."[19]

42. Quest's "Notice of Privacy Policies" contains specifics about the requirements that Quest faces to "maintain the privacy of your PHI."[20] Quest states that "we are required notify affected individuals in the event of a breach involving unsecured protected health information."[21] There is no indication that it has done so.

43. Quest's Notice of Privacy Policies indicates that it may "use an outside collection agency to obtain payment when necessary" and that it would provide protected health information in that instance.[22] These "business associates" are "***required to maintain the privacy and security of PHI***."[23]

44. The requirements—which stem from contractual duties as well as duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")—were not met. Defendants failed to inform specific customers of the data breach and, more importantly, failed to maintain the privacy and security of protected health information.

---

[18] Online Privacy Policy, https://www.questdiagnostics.com/home/privacy-policy/online-privacy.html (last visited June 3, 2019) (emphasis added).
[19] *Id.*
[20] Notice of Privacy Policies, https://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html, (last visited June 4, 2019).
[21] *Id.*
[22] *Id.*
[23] *Id.* (emphasis added).

D. Quest Customers' Information is highly valuable.

45. Defendants were or should have been aware that they were collecting highly valuable data, for which Defendants should have known there is an upward trend in data breaches in recent years.[24]

46. The U.S. Department of Health and Human Services, Office for Civil Rights, currently lists 479 breaches affecting 500 or more individuals in the past 24 months.[25]

47. The co-founder of Lastine, a network security provider, said that "Hackers target financial companies, like this billing collection company, as they often store sensitive financial information that can be turned into immediate gains."[26]

48. Quest knew or should have known that it had an obligation to secure the Reservation Database because it contains highly valuable information.

E. Defendants have harmed Plaintiff by allowing anyone to access their information.

49. Defendants caused harm to Quest customers by failing to prevent hackers from stealing their information. Whether or not their information is subsequently used in a criminal enterprise, the mere theft of PII, PCD, and confidential medical information significantly increases the risk of a customer's identity being exploited in ways that would cause economic

[24] Healthcare Data Breach Statistics, HIPPA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited June 4, 2019) ("Our healthcare statistics clearly show there has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published.").
[25] U.S. Dep't of Health and Human Services, Office for Civil Rights, *Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited June 4, 2019).
[26] Christopher Rowland, Quest Diagnostics discloses breach of patient records, WASH. POST, June 3, 2019, https://www.washingtonpost.com/business/economy/quest-diagnostics-discloses-breach-of-patient-records/2019/06/03/aa37b556-860a-11e9-a870-b9c411dc4312_story.html?utm_term=.78dd30c03a88 (last visited June 3, 2019).

harm, thereby decreasing the value of their PII, and requiring reasonable efforts to mitigate against that risk.

50. Plaintiff and Class Members have a significant, imminent risk of identity theft because of Defendants' actions. Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration date, and other information, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance." In some data breaches, as many as "1 in 4 . . . [eventually] became a victim of identity fraud."

51. Identity thieves can use information from Quest customers to perpetrate a variety of crimes that harm Plaintiff, including immigration fraud; obtaining a driver's license or identification card in the victim's name but with another picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

52. Importantly, reimbursing a consumer for a financial loss due to fraud does not make that individual economically whole. This is so because "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems." In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims."

53. Medical data is particularly valuable to hackers. In June 2016, a hacker reportedly was offering to sell hacked medical records of nearly 700,000 patients for hundreds

of thousands of dollars on a "deep web marketplace."[27] Later, the same hacker revealed that he had a database of 9.3 million records from a U.S. insurer that was for sale.[28]

54. The threat of "medical identity theft" is all too real. In 2010, Experian analyzed the issue and said that, "according to a 2010 Ponemon survey, the average cost incurred in trying to resolve a medical identity theft is more than $20,000. Additionally, 55% of survey respondents had to make out-of-pocket payments to the health plan provider or insurer to restore coverage and 32% experienced an increase in their health insurance premiums."[29]

F. Defendants were on notice for this form of data breach.

55. Confidential medical information is incredibly valuable to hackers. Moreover, as detailed above, health care data breaches are on the rise. Given this fact, Defendants were on notice for the potential harms that could ensue if they failed to protect customers' data.

56. Incredibly, Quest is no stranger to exposing its customers' private information. In late 2016, Quest allowed an unauthorized third party to access its internal internet application and obtained protected health information for 34,000 individuals.[30]

---

[27] Healthcare under Attack: What Happens to Stolen Medical Records?, June 30, 2016, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/healthcare-under-attack-stolen-medical-records (last visited June 4, 2019).

[28] Lording it over the healthcare sector: health insurer database with 9.3M entries up for sale, https://www.databreaches.net/lording-it-over-the-healthcare-sector-health-insurer-database-with-9-3m-entries-up-for-sale/, (last visited June 4, 2019).

[29] Experian, The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches, April 2010, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited June 4, 2019).

[30] http://ir.questdiagnostics.com/news-releases/news-release-details/quest-diagnostics-provides-notice-data-security-incident?ID=2229113&c=82068&p=irol-newsArticle.

57. This data included name, date of birth, lab results, and in some instances, phone numbers.[31] At the time, a company spokesman said that "we're taking it seriously."[32] Notwithstanding this empty promise, less than three years later another set of Quest customers have had their data breached.

CLASS ACTION ALLEGATIONS

58. Plaintiff brings this action on behalf of a class of:

> All individuals who provided information to Quest Diagnostics Incorporated and whose information was provided to American Medical Collection Agency (the "Class").

Plaintiff also brings this action on behalf of a subclass of:

> All individuals who contracted with Quest Diagnostics Incorporated and whose information was provided to American Medical Collection Agency (the "Subclass").

To the extent necessary for manageability at trial, Plaintiff proposes that the Court certify state subclasses in order to group similar causes of action for states requiring similar evidentiary proof. Plaintiff reserves the right to propose these or other subclasses prior to trial.

59. Excluded from the Class and any subclasses are Defendants, and their parents, subsidiaries, agents, officers, and directors. Also excluded is any judicial officer assigned to this case and members of his or her staff.

60. Plaintiff seeks class certification under Rule 23(b)(2) and Rule 23(b)(3) of the Federal Rules of Civil Procedure. In the alterative, he seeks class certification under Rule 23(c)(4) because the below common questions predominate as to particular issues that could

---

[31] *Id.*

[32] Robert Channick, Quest data breach exposes private health information of 34,000 patients, Chicago Tribune, Dec. 13, 2016, https://www.chicagotribune.com/business/ct-quest-data-hack-1214-biz-20161213-story.html.

substantially advance the litigation. The Class meets all express and implied requirements of these rules.

61. **Ascertainability.** The Class is readily ascertainable because it is objectively defined and meets the ascertainability standard of this Circuit. Indeed, the Class consists of individuals whose information was provided to Quest and thus meets the ascertainability standard of every Circuit.

62. **Numerosity—Rule 23(a)(1)**. Defendants admit that a data breach occurred for nearly 12 million Quest customers. Accordingly, the members of the Class are so numerous that joinder of all members is impracticable.

63. **Commonality—Rule 23(a)(2)**. The answer to at least one question common to the Class will drive the resolution of this litigation. For example:

a. Whether Defendants had a duty to take reasonable and prudent security measures.

b. Whether Defendants failed to take reasonable and prudent security measures.

c. Whether Defendants' failure to take reasonable and prudent security measures caused injury.

d. Whether Defendants disclosed Plaintiff's and Class Members' information without their consent.

e. Whether Defendants violated state law when it failed to implement reasonable security procedures and practices.

f. Which security procedures and which notification procedures Defendants should be required to implement.

g. Whether Defendants have a contractual obligation to use reasonable security measures.

h. Whether Defendants have complied with any contractual obligation to use reasonable security measures.

i. What security measures, if any, must be implemented by Defendants to comply with their contractual obligations.

j. Whether Defendants violated state consumer protection and state medical information privacy laws in connection with the actions described herein;

k. Whether Defendants failed to notify Plaintiff and Class Members as soon as practicable and without delay after the data breach was discovered; and

l. Whether Plaintiff and Class Members are entitled to damages, declaratory, or injunctive relief.

64. **Typicality—Rule 23(a)(3).** Plaintiff brings claims for the same type of injury under the same legal theory as the rest of the Class. Among other things, Defendants allowed all Class Members' personal information to be compromised through the same data breach.

65. **Adequacy—Rule 23(a)(4)**. Plaintiff and his counsel are adequate because: (1) there no conflict between the proposed Class representative and other Class members, or, to the extent any conflicts develop, undersigned counsel will propose the appointment of interim class counsel to represent the various Class members' interests; and (2) the proposed Class representatives and their counsel will vigorously pursue the claims of the Class. Plaintiff has no interests contrary to, or in conflict with, the interests of Class Members.

66. **Predominance & Superiority—Rule 23(b)(3)**. Common issues in this litigation predominate over individual issues because those issues discussed in the above

paragraph on commonality are more important to the resolution of this litigation than any individual issues. A class action, moreover, is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiff knows of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action.

67. **Risks of Prosecuting Separate Actions**. This case is appropriate for certification because prosecuting separate actions by individual proposed class members would create the risk of inconsistent adjudications and incompatible standards of conduct for Defendants or would be dispositive of the interests of members of the proposed Class.

68. **Final injunctive relief is appropriate respecting the Class as a whole—Rule 23(b)(2).** Injunctive relief is appropriate because, among other reasons, Defendants' inadequate security exposes all Class Members to a substantial risk of immediate harm. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Negligence

69. Plaintiff incorporates the above allegations as if fully set forth herein.

70. Defendants knew or should have known that AMCA's web payments page was vulnerable to unauthorized access by third parties.

71. Defendants assumed a duty of care to use reasonable means to implement both a policy and process by which it could prevent such unauthorized access. Further, Defendants were responsible for engaging in supervision, monitoring and oversight consistent with the PII, PCD, and confidential medical information that was collected, used, and shared by them.

72. Defendants owed a duty of care to Plaintiff based on obligations created by the HIPAA, which contains specific governmental warnings about the safeguards needed to ensure the confidentiality, integrity, and security of customers' protected medical information.

73. Defendants owed a duty of care to Plaintiff because they collected and stored Plaintiff's and the Class Members' PII, PCD, and confidential medical information and they were foreseeable and probable victims of any inadequate security related policies and practices. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of the Plaintiff and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they would be harmed in the future if Defendants did not protect Plaintiff's and Class Members' information from hackers.

74. Defendants' duties also arose under Section 5 of the Federal Trade Commission Act ("FTC 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 personal and confidential information. Various FTC publications and data security breach orders further form the basis of Defendants' duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

75. Quest acknowledged the need to keep this information secure and stated that "our contractors to who we may provide such information for the limited purpose of providing

services to us ***and who are obligated to keep the information confidential***."[33] Despite this acknowledgment, Quest has not reached out to its customers who had their data breach despite having superior knowledge and being in a position to inform its customers that their data had been hacked.

76. The failure to comply with its Notice of Privacy Practices is just as stark. Quest did not "maintain the privacy" of protected health information, despite acknowledging their legal requirement to do so.[34]

77. Upon information and belief, Defendants improperly and inadequately safeguarded the personal and confidential information of Plaintiff and Class Members in deviation from standard industry rules, regulations, and practices at the time of the data breach.

78. Defendants' failure to take proper security measures to protect Plaintiff's and Class Members' sensitive personal and confidential information has caused Plaintiff and Class Members to suffer injury and damages. As described herein, Plaintiff now must take and have taken affirmative steps to ensure that their identity is not stolen and their financial information is not compromised.

79. Defendants breached these duties in failing to take reasonable measures or to implement reasonable policies and procedures to prevent the unauthorized access to the PII, PCD, and confidential medical information of Plaintiff.

---

[33] Online Privacy Policy, https://www.questdiagnostics.com/home/privacy-policy/online-privacy.html (last visited June 3, 2019) (emphasis added).

[34] Notice of Privacy Policies, https://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html, (last visited June 4, 2019).

80. Defendants further breached these duties in failing to take reasonable measures or to implement reasonable policies and procedures to detect an intrusion into their payment systems for over eight months.

81. Defendants further breached these duties in failing to take reasonable measures or to implement reasonable policies and procedures to notify Plaintiff and Class Members of the data breach.

82. As a result of the breach, Plaintiff suffered damages, and the damages available by way of contract remedies would be inadequate to fully compensate them for their losses.

SECOND CAUSE OF ACTION
Breach Of Contract
(For the Subclass Only)
(Against Quest Only)

83. Plaintiff incorporates the above allegations as if fully set forth herein.

84. Defendant Quest promised to Plaintiff and Subclass Members, through its privacy policy and its contracts with Subclass Members, that it would safeguard Plaintiff's and Class Members' PII, PCD, and confidential medical information. In exchange for that and other promises made by Quest, Plaintiff and Class Members agreed to pay Quest for medical treatment procedures.

85. The Privacy Policy indicates that Quest agreed to properly maintain Plaintiff's and Subclass Members' PII and PCD, enact safeguards to protect the data, and limit access to PII and PCD.

86. Quest breached its promises by failing to safeguard Plaintiff's and Subclass Members' PII, PCD, and confidential medical information, failing to detect the data breach, and failing to notify Plaintiff and Subclass Members in a timely fashion of the data breach.

87. Plaintiff and Subclass Members have performed all, or substantially all, of the obligations imposed on them under the Privacy Policy and their contracts with Quest.

88. Plaintiff and Subclass Members have been damaged as a result of Quest's breach of its promises.

THIRD CAUSE OF ACTION
Unjust Enrichment
(For the Subclass Only)
(Against Quest Only)

89. Plaintiff incorporates the above allegations as if fully set forth herein.

90. Alternatively, if Quest's express promises made in its Privacy Policy do not obligate it to protect Plaintiff's and Subclass Members' information and to timely and accurately notify Plaintiff and Subclass Members if their data had been breached or compromised, then Plaintiff alleges that there exists an implied contract whereby Quest is obligated by the covenant of good faith and fair dealing, to meet those same obligations.

91. If the Court determines that Plaintiff cannot bring a cause of action for breach of contract, Plaintiff asserts a cause of action for the breach of the covenant of good faith and fair dealing.

92. Quest's Privacy Policy contained the implied promise that it would safeguard and limit disclosures of customers' PII, PCD, and confidential medical information. The Privacy Policy contained clear information about the limited purposes that third parties could use the information for.

93. On this basis, Quest informed Plaintiff and Subclass Members that providing their PII, PCD, and confidential medical information would be safe. Plaintiff and Subclass Members accepted these offers made by Quest in allowing Quest to store, maintain, and safeguard their personal and confidential information.

94. When Plaintiff and Subclass Members provided their personal and confidential information to Quest in connection with receiving medical treatment from Quest, they entered into implied contracts with Quest, pursuant to which Quest agreed to safeguard and protect their information, and to timely and accurately notify Plaintiff and Subclass Members if their data had been breached or compromised.

95. Plaintiff and Subclass Members would not have provided to and entrusted their personal and confidential information with Quest in connection with receiving medical treatment in the absence of the implied contract between them.

96. Plaintiff and Subclass Members fully performed their obligations under the implied contract with Quest.

97. Quest breached the implied contract it made with Plaintiff and Subclass Members by failing to safeguard and protect the personal and confidential information of Plaintiff and Subclass Members and by failing to provide timely and accurate notice to them that their information was compromised in and as a result of the data breach.

98. As a direct and proximate result of Quest's breaches of the implied contracts between Quest and Plaintiff and Subclass Members, Plaintiff and Subclass Members sustained actual losses and damages as described in detail herein.

FOURTH CAUSE OF ACTION
Unlawful, Unfair, or Fraudulent Business Practices Under the California Unfair Competition Law
(Cal. Bus. & Prof. Code § 17200, *et seq.*)

99. Plaintiff incorporates the above allegations as if fully set forth herein.

100. California's Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code § 17200, *et seq.*), prohibits any "unlawful, untrue, or fraudulent business act or practices and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

101. Defendants' conduct violated the "unlawful" prong of the UCL by: misrepresenting, actively concealing, and failing to disclose material information regarding the protection of Plaintiff's data.

102. Defendants' conduct also violated the "unfair" prong of the UCL because it was immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the proposed Class members. Defendants have known or should have known since at least August 2018 that Plaintiff's and Class Members' data was breached, and yet Class Members continued to collect and store Class Members' data without adequately warning Plaintiff and Class Members of the data breach. The injury to customers by this conduct greatly outweighs any alleged countervailing benefits to consumers or competition under all circumstances. There is a strong public interest in safeguarding PII, PCD, and confidential medical information. Defendants' conduct was contrary to legislatively declared public policy, as reflected in the CLRA among other legal standards.

103. Defendants' conduct further violated the "fraudulent" prong of the UCL. Defendants' misrepresentations and nondisclosures relating to protecting Plaintiff's and Class Members' data were and are likely to deceive members of the public and did deceive the public. These misrepresentations and nondisclosures were and are material, in that a reasonable person would attach importance to the information and would be induced to act on the information in making purchase decisions. Defendants made these misrepresentations, concealment, and nondisclosures with the intention that consumers would rely on them in their decisions to obtain medical treatment with Quest. Had Plaintiff and the proposed Class Members known about the insufficient security protections on their data that they had provided to Quest, they would not have gone to Quest to obtain medical treatment.

Defendants had exclusive knowledge of the sufficiency of their security protections, such that Plaintiff and the proposed Class Members could not have reasonably avoided their injuries.

104. As a direct and proximate result of Defendants' business practices in violation of the UCL, Plaintiff and the proposed Class Members have suffered injury-in-fact.

105. As a direct and proximate result of Defendants' business practices in violation of the UCL, Defendants have been unjustly enriched and should be required to make restitution to Plaintiff and the proposed Class Members or disgorge its ill-gotten profits pursuant to Sections 17203 of the Business & Professions Code.

106. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiff and the proposed Class Members seek an order of this Court enjoining Defendants from continuing to engage in unlawful, unfair, and fraudulent business practices in violation of the UCL. Plaintiff and the proposed Class Members also seek an order requiring Defendants to disgorge and/or make full restitution of all moneys wrongfully obtained from the Plaintiff and the proposed Class Members. Plaintiff and the proposed Class Members also seek attorney's fees and costs under Cal. Code Civ. Proc. § 1021.5.

FIFTH CAUSE OF ACTION
Violation of the California Confidentiality of Medical Information Act,
(Cal. Civ. Code § 56, *et seq.* (the "CMIA"))

107. Plaintiff incorporates by reference all of the foregoing paragraphs of this Complaint as if fully stated herein.

108. Plaintiff alleges additionally and alternatively that California's CMIA was enacted to protect, among other things, the release of confidential medical information without proper authorization. Cal. Civ. Code §§ 56, *et seq.*

109. To protect the release of this information, the CMIA prohibits entities from negligently disclosing or releasing any person's confidential medical information. Cal. Civ. Code §§ 56.36.

110. The CMIA also creates a duty for entities like Defendants that, "create[], maintain[], preserve[], abandon[], destroy[], or dispose[] of medical information shall do so in a manner that preserves the confidentiality of the information contained herein. Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." Civ. Code Cal. § 101(a).

111. As described herein, Defendants negligently disclosed and released Plaintiff and the proposed Class Members' confidential medical information inasmuch as they failed to implement adequate security protocols to prevent unauthorized access to confidential medical information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data breach or otherwise comply with HIPAA data security requirements.

112. As a direct and proximate result of Defendants' negligence, they disclosed and released Plaintiff and the proposed Class Members' confidential medical information to hackers.

113. Accordingly, Plaintiff and the proposed Class Members seek to recover actual, nominal (include $1,000 nominal damages per disclosure under 56.35(b)), and statutory

damages (including under § 56.36(c)) where applicable, together with reasonable attorneys' fees and costs.

SIXTH CAUSE OF ACTION
Violation of the New Jersey Consumer Fraud Act,
(N.J.S.A. 56:8-1, *et seq.* (the "NJCFA"))

114. Plaintiff incorporates by reference all of the foregoing paragraphs of this Complaint as if fully stated herein.

115. The New Jersey Consumer Fraud Act (the "NJCFA"), N.J.S.A. § 56:8-1, et seq., prohibits the act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise. The NJCFA applies whether or not any person has in fact been misled, deceived or damaged thereby. N.J. Stat. Ann. § 56:8-2.

116. Plaintiff, Defendants, and the proposed Class Members are "persons" within the meaning of N.J. Stat. Ann. § 56:8-1(d).

117. Quest's medical treatments are "merchandise" within the meaning of N.J. Stat. Ann. § 56:8-1(c) because it is an object, ware, good, commodity, or other tangible item offered, directly or indirectly, to the public for sale.

118. At all relevant times material hereto, Defendants conducted trade and commerce in New Jersey and elsewhere within the meaning of the NJCFA. As Defendant Quest is headquartered in New Jersey and Defendants AMCA and Optum360 conduct business in New Jersey.

119. The NJCFA is, by its terms, a cumulative remedy, such that remedies under its provisions can be awarded in addition to those provided under separate statutory schemes.

120. Defendants were engaged in activity "in connection with the sale or advertisement" of "merchandise." Among other things, Defendants advertised and promoted their medical treatments.

121. Prior to Plaintiff and the proposed Class Members' purchase of Quest's medical treatment products, Defendants engaged in deceptive practices that violated the NJCFA. As set forth in detail below, Defendants made statements and omitted material information that had and continue to have the capacity to deceive the public and caused injury to Plaintiff and the proposed Class Members because:

122. Defendants made false or misleading uniform misrepresentations which had the capacity, tendency, and effect of deceiving or misleading consumers.

123. Defendants made uniform representations that they would protect Plaintiff and the proposed Class Members' confidential data that was incorrect.

124. Defendants made uniform representations about the security and safeguards that they undertook that were not in fact true.

125. Defendants failed to disclose the true characteristics and quality of their data security.

126. Defendants advertised Quest's medical treatments with the intent not to sell it as advertised—i.e. with worse data security than advertised.

127. Defendant Quest represented on its website that it is "committed to protecting the privacy of your identifiable health information," when, in fact, Quest failed to safeguard customers' information by providing it to AMCA who had deficient data security protection.

128. Defendants engaged in deception, misrepresentation, knowing concealment, suppression, or omission of material facts with the intent that consumers would rely on the same in connection with the promotion and sale of Quest's medical treatments.

129. Plaintiff and the proposed Class Members reasonably expected that Defendants would protect their confidential PII, PCD, and confidential medical information, and reasonably expected that Defendants would provide truthful statements on their website and privacy policies, and that it would be safe to provide Quest with their information. These representations and affirmations of fact made by Defendants, and the facts they concealed or failed to disclose, are material facts that were likely to deceive reasonable consumers, and that reasonable consumers would, and did, rely upon in deciding whether or not to purchase Quest's medical treatments. Defendants, moreover, intended for consumers, including Plaintiff and the proposed Class Members, to rely on these material facts.

130. In addition to being deceptive, Defendants' misrepresentations active concealment, and failure to disclose material information regarding the defective data security was also unfair, because it was unconscionable, immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to Plaintiff and the proposed Class Members. Defendants have known or should have known since at least since at least August 2018 that Plaintiff's and Class Members' data was breached, and yet Class Members continued to collect and store Class Members' data without adequately warning Plaintiff and Class Members of the data breach. The injury to customers by this conduct greatly outweighs any alleged countervailing benefits to consumers or competition under all circumstances. There is a strong public interest in safeguarding PII, PCD, and confidential medical information. Defendants' conduct was contrary to legislatively declared public policy, as reflected the NJCFA.

131. Defendants took advantage of the inability of the Plaintiff and the proposed Class Members to reasonably protect their interests because of the lack of data security, which Defendants concealed and failed to disclose. Defendants' conduct caused substantial injury to consumers including Plaintiff and the proposed Class Members, which they could not avoid because of Defendants' concealment, as further explained below. The injury to consumers by this conduct greatly outweighs any alleged countervailing benefits to consumers or competition under all circumstances. There is a strong public interest in strong protection of highly confidential and revealing PII, PCD, and medical information. Defendants' conduct was contrary to legislatively declared public policy, including the NJCFA.

132. Defendants had exclusive knowledge that the data security was and is deficient and in violation of HIPAA as set forth above, which gave rise to a duty to disclose these facts to Plaintiff and the proposed Class Members. Specifically, Defendants owed Plaintiff and the proposed Class Members a duty to disclose all the material facts concerning their data security practices because they possessed exclusive knowledge about it, intentionally concealed that knowledge from Plaintiff and the proposed Class Members, and made misrepresentations that were rendered misleading because they were contradicted by withheld facts. Defendants also had an ongoing duty to Plaintiff and the proposed Class Members to refrain from unfair or deceptive practices under the NJCFA in the course of their business. Defendants breached these duties by making misrepresentations and failing to disclose material facts.

133. Plaintiff and the proposed Class Members had no way of discerning that Defendants' representations were false and misleading prior to purchasing Quest's medical treatments, or otherwise learning the facts that Defendants had concealed or failed to disclose

prior to purchasing Quest's medical treatments. Plaintiff and the proposed Class Members did not, and could not, unravel Defendants' deception on their own.

134. Plaintiff and the proposed Class Members reasonably relied upon Defendants' material misrepresentations and nondisclosures. Had Plaintiff and the proposed Class Members known about the deficient data security and accompanying safety risks, they would not have purchased Quest's medical treatments. Plaintiff's and proposed Class Members' reliance on Defendants' concealment and nondisclosures is demonstrated by the fact that Plaintiff and the proposed Class Members purchased Quest's medical treatments with the deficient data security that endangered their health and that rendered a key advertised feature—the level of data security—false, which they would not had they known the truth.

135. As a direct and proximate result of Defendants' misrepresentations, concealment, and failure to disclose material information, Plaintiff and the proposed Class Members have suffered ascertainable loss and actual damages.

136. Defendants' violations present a continuing risk to Plaintiff and the proposed Class Members, as well as to the general public. Defendants' unlawful acts and practices complained of herein affect the public interest.

137. As explained in more detail above, Defendants' conduct was reprehensible.

138. Defendants' poor data security is capable of causing economic harm.

139. Defendants have shown indifference to, and reckless disregard for, the health and safety of Plaintiff and the proposed Class Members because Defendants knew that their data security measures were deficient, but did nothing to protect consumers.

140. Pursuant to N.J. Stat. Ann. § 56:8-19, Plaintiff and the proposed Class Members seek an order enjoining Defendants' violations of the NJCFA and awarding

damages, attorney's fees, and any other just and proper relief available under the NJCFA. Plaintiff and the proposed Class Members also seek punitive and treble damages against Defendants under N.J. Stat. Ann. § 56:8-19.

141. Plaintiff will mail this complaint to the Attorney General within 10 days of filing, pursuant to N.J. Stat. Ann. § 56:8-2.

142. In the event that New Jersey law is not applied, Defendants' actions, as complained of herein, constitute unfair, unconscionable, deceptive or fraudulent acts or practices in violation of the consumer protection statutes of the fifty states.

SEVENTH CAUSE OF ACTION
Declaratory Relief

143. Plaintiff incorporates by reference all factual allegations as if fully set forth herein.

144. There is an actual controversy between Defendants and Class Members concerning whether Defendants have a duty to implement additional safeguards to protect the PII, PCD, and medical information of Plaintiff and Class Members.

145. Pursuant to 28 U.S.C. § 2201, this Court may "declare the rights and legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought."

146. Accordingly, Plaintiff and Class Members seek a declaration that Defendants have a duty to implement safeguards to guard against the future exposure of Plaintiffs' and Class Members' PII, PCD, and confidential medical information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a. Certify this case as a class action, appoint Plaintiff as Class representatives, and appoint Plaintiffs' counsel to represent the Class;

b. Award Plaintiff and Class Members appropriate relief, including actual and statutory damages;

c. Award equitable, injunctive, and declaratory relief as may be appropriate, including without limitation an injunction and an order declaring Defendants' conduct to be unlawful;

d. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

e. Award pre-judgment and post-judgment interest as prescribed by law; and

f. Grant further and additional relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: June 4, 2019

Respectfully submitted,

By: /s/ James E. Cecchi

James E. Cecchi
Caroline F. Bartlett
CARELLA BYRNE CECCHI OLSTEIN BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
Tel.: 973.994.1700
Email: jcecchi@carellabyrne.com
cbartlett@carellabyrne.com

Jason L. Lichtman*
Sean A Petterson*
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

250 Hudson Street, 8th Floor
New York, NY 10013
Telephone: 212.355.9500
Email: jlichtman@lchb.com
spetterson@lchb.com

Michael W. Sobol*
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111
Telephone: 415.956.1000
Email: msobol@lchb.com

Adam J. Levitt*
Amy E. Keller*
DICELLO LEVITT GUTZLER LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602
Telephone: 312.214.7900
Email: alevitt@dicellolevitt.com
akeller@dicellolevitt.com

Attorneys for Plaintiff and the Proposed Class

**Pro hac vice* applications forthcoming