LITE DEPALMA GREENBERG, LLC
Bruce D. Greenberg
570 Broad Street, Suite 1201
Newark, New Jersey 07102
Telephone: (973) 623-3000
Facsimile: (973) 623-0858
bgreenberg@litedepalma.com

Attorneys for Plaintiff and the Proposed Class

[*Additional counsel on signature page*]

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

NOEL BENADOM, individually and on behalf of all those similarly situated, *Plaintiff*, v. QUEST DIAGNOSTICS INC.; and OPTUM360 LLC, *Defendant*.	:	Civil Action No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Noel Benadom ("Plaintiff"), individually and on behalf of classes of similarly situated individuals (the "Classes"), brings this Class Action Complaint against Defendants Quest Diagnostics Inc., and Optum 360, LLC (collectively "Defendants"). Plaintiff alleges as follows upon personal knowledge as to his own acts and experience, and upon information and belief and the investigation of his attorneys as to all other matters:

I. NATURE OF THE CASE

1. Plaintiff brings this class action lawsuit on his behalf, and on behalf of Classes of similarly situated individuals, against Defendants for their failure to protect the confidential information of millions of consumers—including Personally Identifiable Information ("PII"), first and last names, dates of birth, addresses, telephone numbers, social security numbers, dates

of service, Protected Health Information ("PHI"), provider names, payment balance information, credit cards or bank account information, and other confidential information (collectively, "Sensitive Information").

2. On June 3, 2019, Quest Diagnostics Inc. ("Quest") publicly announced that its customers' Sensitive Information was subject to unauthorized access by third parties between August 1, 2018 and March 30, 2019 due to a data security breach (the "Data Breach") of its billing collections vendor, Retrieval-Masters Creditor's Bureau, Inc., d/b/a American Medical Collection Agency ("AMCA").

3. On or around May 14, 2019, AMCA notified Quest and Quest's revenue cycle management provider Optum360, LLC ("Optum360"), that there was a Data Breach of AMCA's web payment page. According to AMCA, the Data Breach began on August 1, 2018, and thereafter went undetected until March 30, 2019. After discovering the Data Breach, AMCA waited months before notifying affected individuals, preventing Plaintiff and the proposed Classes from taking steps to prevent the further actual and potential misuse of their Sensitive Information.

4. AMCA's affected systems contained Quest's customers' Sensitive Information.

5. As of May 31, 2019, AMCA believed that the Data Breach affected the Sensitive Information of 11.9 million Quest customers.

6. At all relevant times, Quest promised and agreed—throughout its Notice of Privacy Practices and other written assurances—to safeguard and protect Sensitive Information in accordance with Health Insurance Portability and Accountability Act ("HIPAA") regulations, federal, state and local laws, and industry standards. In addition, Quest promised and agreed that

their contracted service providers and other business associates, such as billing services providers, are "required to maintain the privacy" and security of PHI.[1]

7. Plaintiff and the Classes would not have provided their Sensitive Information to Defendant, if Plaintiff and Class members knew that Defendants would breach its promises and agreements by failing to ensure that its vendors used adequate security measures and/or provide their customers' Sensitive Information, including PII, to business associates that utilized inadequate security measures and also by providing customers' Sensitive Information to business associates that utilized inadequate security measures.

8. Defendants' failure to ensure that its vendors implemented adequate security protocols compromised the Sensitive Information of millions of consumers, including Plaintiff and the Classes, fell well short of Defendants' agreements and obligations, and also fell short of Plaintiff's and other Class members' reasonable expectations for protection of the Sensitive Information provided to Quest.

9. As a result of Defendants' conduct and the ensuing Data Breach, Plaintiff and the members of the proposed Classes have suffered actual damages, and are at imminent risk of future harm, including identity theft and fraud that could result in further monetary loss. Accordingly, Plaintiff brings suit, on behalf of himself and Classes of all others similarly situated, to seek redress for Defendants' unlawful conduct.

II. PARTIES

A. Plaintiff Noel Benadom

10. Plaintiff Noel Benadom is a citizen and resident of the State of Florida.

[1] Notice of Privacy Practices, Quest Diagnostics, https://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html (last visited June 14, 2019).

11. Plaintiff Benadom went to a Quest laboratory to obtain medically prescribed blood testing in or around 2015 and 2016.

12. Plaintiff Benadom provided Quest with Sensitive Information, including medical information and PII, as well as credit card information, as part of obtaining laboratory testing services from Quest.

13. A bill for services allegedly performed by Quest, and allegedly in Plaintiff Benadom's name, was sent to AMCA for collection.

14. In June 2019, Plaintiff Benadom received a notification letter from AMCA regarding the Data Breach. Upon information and belief, Plaintiff Benadom's Sensitive Information, including PII and financial information, was compromised in the Data Breach of Quest's billing service provider, AMCA.

15. Plaintiff Benadom experienced fraud around the time the Data Breach. On or around May 20, 2019, Plaintiff Benadom was contacted regarding a fraudulent attempt someone had made to make travel reservations through Orbitz.com in Plaintiff Benadom's name with one of Plaintiff Benadom's old payment cards.

B. Defendant Quest Diagnostics Inc.

16. Defendant Quest Diagnostics Inc. is a corporation existing under the laws of the State of Delaware with its headquarters and principal place of business located in Secaucus, New Jersey.

C. Defendant Optum360, LLC

17. Optum360, LLC is a corporation existing under the laws of the State of Delaware with its principal place of business in Eden Prairie, Minnesota.

III. JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2) because (a) at least one member of the putative Class is a citizen of a state different from at least one Defendant, and (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

19. This Court has personal jurisdiction over Defendants because they are registered to and regularly do conduct business in this District, and a substantial part of the conduct alleged in this Complaint occurred in, was directed to, and/or emanated, in part, from this District.

20. Venue is proper pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the conduct alleged in this Complaint occurred in, were directed to, and/or emanated from this District. Venue is additionally proper because Defendants are registered to and do conduct business in this District, and because Defendant Quest's principal place of business is located in this District.

IV. FACTUAL BACKGROUND

A. Quest Obtained Sensitive Information from Plaintiff and the Putative Class and Shared that Information with AMCA and Optum360.

21. Quest is "the world's leading provider of diagnostic information services."[2] Quest generated revenues of approximately $7.53 billion in 2018. Quest operates nationally, and annually serves one in three adult Americans and half the physicians and hospitals in the United States.[3]

[2] *Fact Sheet*, Quest Diagnostics, http://newsroom.questdiagnostics.com/index.php?s=30664 (last visited June 14, 2019).

[3] *Id.*

22. Quest offers a variety of laboratory testing services to patients, including Plaintiff Benadom and the putative Classes, following an order from a physician. Quest's clinical laboratory testing services include: blood tests, body fluid testing, tissue pathology and cytology, health screening and monitoring tests, drug screening and testing as well as genetic testing.[4]

23. Quest operates approximately 2,200 "Patient Service Centers" throughout the U.S. at which it performs laboratory testing services. Patients may have their specimens collected for testing either at their physician's office or in one of Quest's patient service centers.[5]

24. For appointments at its Patient Service Centers, Quest requires patients, such as Plaintiff Benadom and the putative Classes, to bring with them and provide to Quest the lab order from the patient's doctor, photo identification, and current health insurance information.[6]

25. Quest Diagnostics also obtains "diagnosis information from the ordering physicians [sic] office."[7]

26. Quest charges for the laboratory services it provides to patients. The invoices Quest sends are for laboratory testing fees, and these are "separate from any bill [patients] may have received from [their] physician."[8] Patients whose insurance does not cover the services and uninsured patients are responsible for payment.

---

[4] *Frequently Asked Questions – Laboratory Testing*, Quest Diagnostics, https://www.questdiagnostics.com/home/patients/about-testing/faqs.html#requesting1 (last visited June 14, 2019).

[5] *Company Information*, Quest Diagnostics, http://newsroom.questdiagnostics.com/company-information (last visited June 14, 2019).

[6] *Preparing for a lab test: getting started*, Quest Diagnostics, https://www.questdiagnostics.com/home/patients/preparing-for-test/get-started (last visited June 14, 2019).

[7] Frequently Asked Questions: Billing Services, Quest Diagnostics, https://billing.questdiagnostics.com/PatientBilling/PATFaqExternal.action?getLabCode=false&fromLink=doFaq (last visited June 14, 2019).

[8] *Id.*

27. When a Quest invoice is unpaid within the requested time period, Quest will refer the invoice to a collection agency. Quest partners with Optum360 for assistance with Quest's billing and bill collection processes. AMCA provides billing collections services to Optum360, which in turn is a Quest contractor.[9]

28. Upon information and belief, Quest, through its contractor Optum360, provided AMCA with Sensitive Information about Quests' patients, including Plaintiff Benadom and the putative Classes, in order to facilitate the bill collection process.

29. The patient information Quest provided to AMCA contained Sensitive Information that included personal and medical information, such as the first and last name, date of birth, address, phone, date of service, service provider, and account balance information, and social security numbers.[10]

30. Upon information and belief, AMCA stored the information Quest provided to AMCA in its own computer systems. These same AMCA systems were compromised in the Data Breach.

31. In addition, AMCA also obtains Sensitive Information from the Quest patients from whom AMCA seeks to collect payments. This information includes financial information, such as credit card or bank account information. Upon information and belief, AMCA stored this information in the computer systems compromised in the Data Breach.

---

[9] *Update on American Medical Collection Agency breach: Almost 12 million Quest Diagnostic patients impacted*, DataBreaches.net (June 3, 2019), https://www.databreaches.net/update-on-american-medical-collection-agency-breach-almost-12-million-quest-diagnostic-patients-impacted/ (last visited June 14, 2019).

[10] Quest Diagnostics Form 8-K (June 4, 2019), https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm

B. Defendants Had a Duty and Obligation to Protect Plaintiff's and Class Members' Sensitive Information from Unauthorized Disclosure.

32. Defendants agreed, and had a duty and obligation, to keep confidential the Sensitive Information their patients disclosed to them and to protect this information from unauthorized disclosure. Defendants' agreement, duties, and obligations are based on: (1) HIPAA; (2) industry standards; and (3) the agreements and promises made to Plaintiff and the putative Classes. Class members provided their Sensitive Information to Defendants with the reasonable belief that Defendants and their business affiliates would comply with their agreements and any legal requirements to keep that Sensitive Information confidential and secure from unauthorized disclosure.

33. HIPAA requires that Quest provide every patient it treats, including Plaintiff and the putative Class members with a privacy notice.

34. In this HIPAA-mandated privacy notice, Quest agrees that its patients it will keep PHI of its patients, including Plaintiff Benadom and the putative Classes, confidential and protected from unauthorized disclosure. In its Notice of Privacy Practices effective April 12, 2018, Quest promises and agrees in relevant part[11]:

> Quest Diagnostics and its wholly owned subsidiaries (collectively "Quest Diagnostics") are committed to protecting the privacy of your identifiable health information. This information is known as "protected health information" or "PHI." PHI includes laboratory test orders and test results as well as invoices for the healthcare services we provide.
>
> * * *

[11] *Notice of Privacy Practices*, Quest Diagnostics, https://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html (last visited June 14, 2019).

> **Our Responsibilities**
>
> Quest Diagnostics is required by law to maintain the privacy of your PHI. We are also required to provide you with this Notice of our legal duties and privacy practices upon request. It describes our legal duties, privacy practices and your patient rights as determined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). We are required to follow the terms of this Notice currently in effect.
>
> * * *
>
> **Payment**
>
> Quest Diagnostics will use and disclose your PHI for purposes of billing and payment. For example, we may disclose your PHI to health plans or other payers to determine whether you are enrolled with the payer or eligible for health benefits or to obtain payment for our services. If you are insured under another person's health insurance policy (for example, parent, spouse, domestic partner or a former spouse), we may also send invoices to the subscriber whose policy covers your health services.
>
> * * *
>
> **Business Associates**
>
> We may provide your PHI 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. For example, we may provide information to companies that assist us with billing of our services. We may also use an outside collection agency to obtain payment when necessary.

35. Quest posts the same Notice of Privacy Practices on its website, acknowledging its agreement, duty, and promise to protect all Sensitive Information in its possession.

36. Quest also has an Online Privacy Policy where it makes additional promises to its customers regarding the privacy of their Sensitive Information[12]:

[12] Online Privacy Policy, Quest Diagnostics, https://www.questdiagnostics.com/home/privacy-policy/online-privacy.html (last visited June 14, 2019).

> **How We Protect Information Online**
>
> We exercise great care to protect your personal information. This includes, among other things, using industry standard techniques such as firewalls, encryption, and intrusion detection. As a result, while we strive to protect your personal information, we cannot ensure or warrant the security of any information you transmit to us or receive from us. This is especially true for information you transmit to us via email since we have no way of protecting that information until it reaches us since email does not have the security features that are built into our websites.
>
> In addition, 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. We educate our employees about the importance of maintaining confidentiality of customer information.
>
> * * *
>
> **Disclosure of Personal Information to Third Parties**
>
> We will not disclose any personal information to any third party (excluding our contractors to whom we may provide such information for the limited purpose of providing services to us and who are obligated to keep the information confidential), unless (1) you have authorized us to do so; (2) we are legally required to do so, for example, in response to a subpoena, court order or other legal process and/or, (3) it is necessary to protect our property rights related to this website. We also may share aggregate, non-personal information about website usage with unaffiliated third parties. This aggregate information does not contain any personal information about our users.

37. Quest's data security agreement, obligations, and commitments are particularly important given the substantial increase in data breaches (particularly in the healthcare industry) during the period preceding the Data Breach. Quest's failure to provide the data-security protections they committed to provide to Plaintiff and members of the putative Classes was particularly egregious in light of specific government warnings regarding the possibility of attempts to hack companies like Quest. Such warnings alerted Quest of the risk of a data breach and further emphasized Quest's duty to keep patients' Sensitive Information secure.

38. For example, on April 8, 2014, the Federal Bureau of Investigation's Cyber Division issued a Private Industry Notification to companies within the healthcare sector, stating that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and pointed out that "[t]he biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise." The same warning specifically noted that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or PII."[13]

39. AMCA was a "business associate" of Quest and Optum360, with whom these entities shared Sensitive Information. As Quest's and Optum360's business associate, AMCA was required to maintain the privacy and security of Plaintiff's and Class members' Sensitive Information. HIPAA mandates that a covered entity may disclose PHI to a "business associate" only if the entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[14]

C. Defendants Failed to Properly Protect Plaintiff's and the Putative Class' Sensitive Information.

40. Between August 1, 2018 and March 30, 2019, an unauthorized user gained access to the AMCA system that contained information obtained from various entities, including Defendants Quest, and Optum360, as well as information that AMCA collected itself.

---

[13] *(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (Apr. 8, 2014), FBI Cyber Division Private Industry Notification, *available at* https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf. .

[14] *See* 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e).

41. The length of time between the breach and AMCA's discovery indicates that AMCA's systems to detect intrusion, detect unusual activity, and log and report such events was inadequate. For example, according to technology-security company FireEye, the median amount of time between when a data breach occurs and when it is detected was 78 days in 2018. This number has consistently been on a downward trend in recent years.[15] The fact that it took AMCA 242 days to detect the Data Breach is evidence of its failure to employ reasonable, industry-standard data-security practices to safeguard Plaintiff's and Class members' Sensitive Information.

42. AMCA's apparent inability to detect the Data Breach on its own, when a third-party security firm (Gemini Advisory—which was *not* working for AMCA) was apparently able to do so with ease, is further evidence of the fact that AMCA employed inadequate data-security practices.

43. On February 28, 2019, Gemini Advisory identified a large number of compromised payment cards while monitoring dark web marketplaces where payment-card data, and associated PII, is bought and sold. Almost 15% of these records of compromised payment cards included additional PII, such as dates of birth, Social Security numbers, and physical addresses. A thorough analysis indicated that the information was likely stolen from the online portal of AMCA, one of the largest recovery agencies for patient collections. Several financial institutions also collaboratively confirmed the connection between the compromised payment card data and the breach at AMCA.[16]

---

[15] *M-Trends 2019: FireEye Mandiant Services Special Report*, *available at* https://content.fireeye.com/m-trends (last visited June 11, 2019).

[16] *American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory*, DataBreaches.net (May 10, 2019), https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/.

44. "On March 1, 2019, Gemini Advisory attempted to notify AMCA," but as Gemini Advisory reportedly told DataBreaches.net, "they did not get any response to phone messages they left." Failing to obtain any response from AMCA, Gemini Advisory promptly contacted federal law enforcement, which reportedly followed up by contacting AMCA."[17]

45. Following notification from law enforcement, AMCA's payment portal became unavailable for weeks.[18]

46. Quest announced in its June 4, 2019 filing with the SEC that:

> AMCA first notified Quest and Optum360 on May 14, 2019 of potential unauthorized activity on AMCA's web payment page. On May 31, 2019, AMCA notified Quest and Optum360 that the data on AMCA's affected system included information regarding approximately 11.9 million Quest patients. AMCA believes this information includes personal information, including certain financial data, Social Security numbers, and medical information, but not laboratory test results.[19]

47. As Quest further stated in its SEC filing 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).[20]

48. In a written statement attributed to AMCA, AMCA announced it was still investigating the breach:

---

[17] *Id.*

[18] *Id.*

[19] Quest Form 8-K (June 4, 2019), https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm; *see also News Release: Quest Diagnostics Statement on the AMCA Data Security Incident*, Quest Diagnostics (June 3, 2019), http://newsroom.questdiagnostics.com/AMCADataSecurityIncident; Brian Krebs, *LabCorp: 7.7 Million Consumers Hit in Collections Firm Breach*, Krebs on Security (June 4, 2019), https://krebsonsecurity.com/2019/06/labcorp-7-7m-consumers-hit-in-collections-firm-breach/

[20] *Id.*

> We are investigating a data incident involving an unauthorized user accessing the American Medical Collection Agency system," reads a written statement attributed to the AMCA. "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.
>
> . . . .
>
> We hired a third-party external forensics firm to investigate any potential security breach in our systems, migrated our web payments portal services to a third-party vendor, and retained additional experts to advise on, and implement, steps to increase our systems' security. We have also advised law enforcement of this incident. We remain committed to our system's security, data privacy, and the protection of personal information.[21]

49. Since learning of the breach, Quest has suspended referring past due accounts to AMCA.[22] "Quest says it has since stopped doing business with the AMCA and has hired a security firm to investigate the incident."[23]

50. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS").

---

[21] *LabCorp: 7.7 Million Consumers Hit in Collections Firm Breach*, Krebs on Security (June 4, 2019), https://krebsonsecurity.com/2019/06/labcorp-7-7m-consumers-hit-in-collections-firm-breach/; *see also Information about the AMCA Data Security Incident*, LabCorp, https://www.labcorp.com/AMCA-data-security-incident (last updated June 10, 2019).

[22] *Unsurprisingly, big numbers from the AMCA breach are starting to be revealed*, DataBreaches.net (June 4, 2019), https://www.databreaches.net/unsurprisingly-big-numbers-from-the-amca-breach-are-starting-to-be-revealed/

[23] Brian Krebs, *LabCorp: 7.7 Million Consumers Hit in Collections Firm Breach*, Krebs on Security (June 4, 2019), https://krebsonsecurity.com/2019/06/labcorp-7-7m-consumers-hit-in-collections-firm-breach/

PCI DSS is the industry standard governing the security of payment card data, although it sets the minimum level of what must be done, not the maximum.

51. The payment card industry has published a guide on point-to-point encryption and its benefits in securing payment card data: "point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[24] Had AMCA implemented a P2PE solution prior to the data breach and an attacker were to steal encrypted payment card data, that data would have been commercially worthless to the attacker as the attacker would not be able to decrypt the data to obtain the information necessary to make fraudulent purchases.

52. Gemini Advisory found credit card numbers from the breach for sale on the dark web, which means that AMCA did not encrypt those numbers in accordance with PCI DSS.

53. Access to the 11.9 million Quest patient records through AMCA's online portal would not have been possible had AMCA maintained appropriate protections. The sheer number of records suggests that AMCA was not destroying or archiving inactive records such as Plaintiff's so that they could not be accessed through the internet, a standard practice that likely would have greatly reduced the number of people impacted by this breach.

[24] Securing Account Data with the PCI Point –to-Point Encryption Standard v2, available at https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf (last accessed June 11, 2019).

D. Data Security Breaches Lead to Increased Actual and Potential Identity Theft.

54. Defendants knew or should have known that the Sensitive Information that they were collecting from Plaintiff and members of the putative Classes, which was stolen during the Data Breach, was highly valuable and highly sought-after by criminals.

55. 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]

56. The United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report") that identity thieves use personally identifying data to open financial accounts, receive government benefits and incur charges and credit in a person's name.[26] As the GAO Report notes, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

57. In addition, the GAO Report makes clear that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[27]

58. Identity theft victims must often spend countless hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such

---

[25] *Healthcare Data Breach Statistics*., HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited June 10, 2019).

[26] *See Personal Information: Data Breaches Are Frequent, But Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* http://www.gao.gov/new.items/d07737.pdf.

[27] *Id*.

as social security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[28]

59. With access to an individual's Sensitive Information, criminals can do more than just empty a victim's bank account; they can also commit many types of fraud, including: obtaining a driver's license or other official identification card in the victim's name but with the thief's picture on it; using the victim's name and social security number to obtain government benefits; and filing a fraudulent tax return using the victim's PII. In addition, identity thieves may obtain a job using the victim's PII, rent a house or receive medical services, prescription drugs and goods, and cause fraudulent medical bills to be issued in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued against the identity theft victim.[29] Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail and other negative effects.

60. In a data breach implicating a medical provider or medical information, consumers face the additional risk of their Health Savings Accounts ("HSAs") being compromised. HSAs are often tied to specialized debit cards used to make medical-based

[28] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[29] *See Warning Signs of Identity Theft*, Federal Trade Commission, *available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft#What (last visited June 13, 2019).

payments. However, they can also be used for regular purchases (albeit incurring a severe tax penalty).[30] Such information is an "easy target" for criminal actors.[31]

61. Sensitive Information is a valuable commodity to identity thieves. Compromised Sensitive Information is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, social security numbers and other Sensitive Information directly on various dark web[32] sites making the information publicly available.[33]

62. Further, medical databases are particularly high value targets for identity thieves. According to one report, a stolen medical identity has a $50 street value on the black market, whereas a Social Security number sells for only $1.[34]

63. The medical industry has experienced disproportionally higher instances of data breaches than any other industry.[35]

---

[30] *American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory*, DataBreaches.net (May 10, 2019), https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/.

[31] *Id.*

[32] The dark web refers to encrypted content online that cannot be found using conventional search engines and can only be accessed through specific browsers and software. MacKenzie Sigalos, *The dark web and how to access it* (Apr. 14, 2018), https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html (last accessed June 17, 2019).

[33] *Here's How Much Your Personal Information Is Selling for on the Dark Web* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 17, 2019); McFarland et al., *The Hidden Data Economy*, at 3, *available at* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf (last visited June 17, 2019).

[34] *Study: Few Aware of Medical Identity Theft Risk*, Claims Journal (June 14, 2012), https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited June 10, 2019).

[35] Bob Kehoe, *Hospitals boost efforts to improve cybersecurity*, Health Facilities Management, (April 26, 2016), https://www.hfmmagazine.com/articles/2162-hospitals-boost-efforts-to-improve-cybersecurity?dcrPath=%2Ftemplatedata%2FHF_Common%2FNewsArticle%

E. Plaintiff and Putative Class Members Are in Imminent Danger of Identity Theft.

64. Defendants caused harm to Plaintiff and putative Class members by sharing their Sensitive Information with AMCA. Quest failed to properly monitor its vendor, and AMCA failed to prevent attackers from accessing and stealing this information in the Data Breach.

65. Criminals steal—and sell—Sensitive Information in order to use it for illicit means. The question is when, not whether, it will be misused. But whether or not the Sensitive Information stolen in the Data Breach is later used in a criminal enterprise, Plaintiff and putative Class members suffered economic harm as even the mere theft of their Sensitive Information significantly increases the risk of their identity being exploited in ways that can cause economic harm to them. This increased risk decreases the value of their Sensitive Information.

66. Plaintiff and members of the putative Classes have experienced fraud at or near the time of the announced Data Breach, including Plaintiff Benadom.

67. In or around May 2019, Plaintiff Benadom was contacted regarding a fraudulent attempt someone had made to make travel reservations in Plaintiff Benadom's name with one of Plaintiff Benadom's old payment cards. Plaintiff Benadom provided Defendant Quest with payment card information in connection with paying for laboratory testing services.

V. CLASS ALLEGATIONS

68. Plaintiff Benadom brings this action on behalf of a Nationwide Class and Florida Subclass, defined respectively as follows:

2Fdata%2FHFM%2FHFM-Daily%2F2016%2Fibm-cybersecurity-intelligence-index-health-care (noting that a report from IBM Security "noted that in 2015, health care became the most frequently attacked field, moving ahead of manufacturing and financial services"); *The Healthcare Industry – A Prime Target for Hackers and Data Breaches*, Bluefin, https://www.bluefin.com/bluefin-news/the-healthcare-industry-a-prime-target-for-hackers-and-data-breaches/ (last visited June 12, 2019) ("healthcare is now the most heavily attacked industry").

> Quest Nationwide Class: All persons in the United States who were charged for services from Quest and whose Sensitive Information was maintained on the AMCA systems that were compromised as a result of the Data Breach announced by Quest on or around June 3, 2019.
>
> Quest Florida Subclass: All residents of Florida who were charged for services from Quest and whose Sensitive Information was maintained on the AMCA systems that were compromised as a result of the Data Breach announced by Quest on or around June 3, 2019.

69. To the extent necessary for manageability, Plaintiff proposes, in the alternative to the Nationwide Class, that the Court certify state subclasses that would group together similar causes of action for states requiring similar evidentiary proof. Plaintiff reserves the right to amend the Class definitions if discovery and further investigation reveal that the Classes should be expanded, divided into further subclasses, or modified in any other way. Plaintiff reserves the right to propose other subclasses prior to trial.

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

71. Plaintiff seeks class certification pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3). In the alternative, Plaintiff seeks class certification under Fed. R. Civ. P. 23(c)(4) because the common questions listed herein predominate as to particular issues that could substantially advance the litigation. The proposed Classes meet the applicable requirements for certification under Fed. R. Civ. P. 23.

72. **Numerosity**: According to Defendants' public statements, there are approximately 11.9 million individuals in the Quest Nationwide Class. As a result, there are likely thousands of individuals in the Subclass, making joinder of each individual member

impracticable. Ultimately, members of the Classes will be easily identified through Defendants' records.

73. **Commonality and Predominance**: Questions of law and fact common to the claims of Plaintiff and the other members of the Classes predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include:

a. Whether Defendants failed to adequately safeguard Plaintiff's and the Classes' Sensitive Information;

b. Whether Defendants failed to protect or otherwise keep Plaintiff's and the Classes' Sensitive Information secure, as promised;

c. Whether Defendants' storage of Plaintiff's and the Classes' Sensitive Information violated HIPAA, federal, state, local laws, or industry standards;

d. Whether Defendants engaged in unfair or deceptive practices by failing to properly safeguard Plaintiff's and the Classes' Sensitive Information, as promised;

e. Whether Defendant violated the consumer protection statutes applicable to Plaintiff and the Classes;

f. Whether Defendants failed to notify Plaintiff and members of the Classes about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

g. Whether Defendants acted negligently in failing to safeguard Plaintiff's and the Classes' Sensitive Information;

h. Whether Plaintiff and the members of the Classes are entitled to damages as a result of Defendants' conduct.

74. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Classes. Plaintiff and the members of the Classes sustained damages as a result of Defendants' uniform wrongful conduct during transactions with them, including their storage and transmission of the Sensitive Information and failure to adequately safeguard it.

75. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Classes and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Classes, and Defendants have no defenses unique to Plaintiff. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Classes and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to those of the other members of the Classes.

76. **Risks of Prosecuting Separate Actions**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendants or would be dispositive of the interests of members of the proposed Classes.

77. **Policies Generally Applicable to the Classes**: This class action is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to Plaintiff and proposed Classes as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Classes and making final injunctive relief appropriate with respect to the proposed Classes as a whole. Defendants' lax data security protocols and practices challenged herein apply to and affect the members of the Classes uniformly, and Plaintiff's challenges to those practices hinge on Defendants' conduct

with respect to the proposed Classes as a whole, not on individual facts or law applicable only to Plaintiff.

78. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Classes. The injuries suffered by each individual member of the Classes are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendants' conduct. Absent a class action, it would be virtually impossible for individual members of the Classes to obtain effective relief from Defendants. Even if members of the Classes could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

VI. CAUSES OF ACTION

FIRST CLAIM FOR RELIEF

Negligence
(Against All Defendants on Behalf of Plaintiff and the Nationwide Class)

79. Plaintiff incorporates paragraphs 1 – 67 as if fully set forth herein.

80. Defendants required Plaintiff and the Class members to submit Sensitive Information in order to obtain services and in consideration for Plaintiff and Class members paying for or using those services.

81. By collecting and storing this data, and by sharing this data with their business associates, Quest had a duty of care to use reasonable means to secure and safeguard this

Sensitive Information, to prevent disclosure of the information from itself and its vendors, and to guard the information from theft.

82. Defendants Quest and Optum360 assumed a duty of care to use reasonable means and implement policies and procedures to prevent unauthorized access to this Sensitive Information.

83. Defendants Quest and Optum360 had a duty to monitor, supervise, or otherwise provide oversight to safeguard the Sensitive Information they stored and shared with their business associates and vendors.

84. Furthermore, given the other major data breaches affecting the healthcare and financial industries, Plaintiff and the Class members are part of a well-defined, foreseeable, finite, and discernible group that was at high risk of having their Sensitive Information stolen.

85. Defendants Quest and Optum360 owed a duty to Plaintiff and members of the Class to provide security consistent with industry standards, statutory requirements, and the other requirements discussed herein, and to ensure that their systems and networks—and the personnel responsible for them—adequately protected their patients' or customers' Sensitive Information.

86. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiff or the other Class members, on the other hand. The special relationship arose because Plaintiff and the members of the Classes entrusted Defendants with their Sensitive Information as part of receiving or paying for laboratory services. Defendants alone were in a position to ensure that their systems, as well as those of its vendors and business associates, were sufficient to prevent or minimize the Data Breach.

87. Defendants' duty to use reasonable security measures also arose under HIPAA, pursuant to which Defendants were required to "reasonably protect" PHI 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). Plaintiff's and Class members' Sensitive Information that was compromised in the Data Breach includes PHI, such as provider names, dates of service, medical billing information and potentially other "protected health information" within the meaning of HIPAA.

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

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

90. Defendants knew or should have known that AMCA's web payments page was vulnerable to unauthorized access.

91. Defendants breached their common law, statutory and other duties—and thus, were negligent—by failing to use reasonable measures to protect consumers' Sensitive Information from hackers, failing to limit the severity of the Data Breach, and failing to detect the Data Breach in a timely fashion.

92. It was foreseeable that Defendants' failure to use reasonable measures to protect consumers' Sensitive Information, including PII, from hackers, failure to limit the severity of the Data Breach, and failure to detect the Data Breach in a timely fashion, would result in injury to Plaintiff and the members of the Classes. Further, the breach of security, unauthorized access, and resulting injuries to Plaintiff and the Classes were reasonably foreseeable, particularly in light of the other major data breaches affecting the healthcare and financial industries.

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

94. Accordingly, Plaintiff, on behalf of himself and members of the Class, seeks an order declaring that Defendants' conduct constitutes negligence, and awarding damages in an amount to be determined at trial.

SECOND CLAIM FOR RELIEF

Violation of New Jersey Consumer Fraud Act,
N.J.S.A. 56:8-1, *et seq.*
(Against Defendant Quest on behalf of Plaintiff and the Nationwide Class)

95. Plaintiff incorporates paragraphs 1–67 as if fully set forth herein.

96. The New Jersey Consumer Fraud Act 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 . . . ." N.J.S.A. 56:8-2.

97. At all relevant times material hereto, Quest conducted trade or commerce, or furnished services in the State of New Jersey.

98. Plaintiff, Defendant, and the proposed Class Members as "persons" within the meaning of N.J.S.A. 56:8-1(d).

99. Quest's medical treatments are "merchandise" within the meaning of N.J.S.A. 56:8-1(c) because they are "objects, wares, goods, commodities, services or anything offered, directly or indirectly to the public for sale."

100. Quest, while conducting trade or commerce or furnishing services in the State of New Jersey, engaged in deceptive acts and practices in violation of N.J.S.A. 56:8-2, because:

a. Defendant failed to enact adequate privacy and security measures to protect the Class Members' Sensitive Information from unauthorized disclosure, release, data breach or theft;

b. Defendant failed to take proper action to address known security risks;

c. Defendant made false or misleading misrepresentations that it would maintain adequate data privacy and security practices and procedures to safeguard the Sensitive Information from unauthorized disclosure, release, data breach or theft;

d. Defendant failed to disclose, omitted, actively concealed the material fact of the inadequacy of its data security or the true characteristics and quality of their data security;

e. Defendant failed to disclose, omitted, actively concealed the material fact of its reliance on AMCA's inadequate data security; and

f. Defendant made false or misleading misrepresentations that that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Sensitive Information including but not limited to duties imposed by HIPAA.

101. The above listed acts were deceptive because they were likely to mislead a reasonable consumer acting reasonably under the circumstances, and such acts were immoral, unethical, oppressive, unscrupulous, unconscionable, and substantially injurious to Plaintiff and Class members.

102. As set out above, because only Defendant knew (or should have known) that it were not complying with its own data security representations and obligations, there was no way for members of the public, including Plaintiff and members of the Classes, to avoid the injury caused by Defendant's conduct. Defendant's failure to use adequate data security practice and failure live up to its data security representations and obligations did not create any countervailing benefits.

103. Plaintiff and Class members reasonably expected that Defendant would protect their Sensitive Information and provide truthful statements regarding their privacy policies.

104. Defendant engaged in omission of material facts, deception, active concealment, and misrepresentation with the intent that Plaintiff and the putative Classes would rely on the same when providing Sensitive Information to Defendant.

105. Defendant's failure to disclose its actual (and substandard) security practices substantially injured the public because it caused millions of consumers to enter into transactions they otherwise would not have, and because it compromised the integrity of Plaintiff's and the Classes Sensitive Information. Further, Defendant's use of substandard security did not create any benefits sufficient to outweigh the harm it caused.

106. Defendant's deceptive acts or practices and general course of conduct is injurious to the public interest, and such acts are ongoing and/or have a substantial likelihood of being repeated inasmuch as the long-lasting harmful effects of their misconduct may last for years (e.g., affected individuals could experience identity theft for years). As such, Defendant's violations present a continuing risk to Plaintiff and the proposed Class members, as well as to the general public.

107. As a result of Defendant's conduct, Plaintiff and members of the Classes have suffered actual damages, including the lost value of their Sensitive Information; the lost value of their personal data and lost property in the form of their breached and compromised Sensitive Information (which is of great value to third parties); ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports;

expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

108. Plaintiff seeks relief under N.J.S.A. 56:8-2, 56:8-19, including but not limited to actual damages in an amount to be proven at trial, treble damages, and reasonable attorney's fees and costs. The amount of such damages is to be determined at trial.

109. Plaintiff also seeks to enjoin Defendant, pursuant to N.J.S.A. 56:8-19, from its deceptive acts and practices described above. Each Class Member will be irreparably harmed unless the Court enjoins Defendant's unlawful, deceptive actions in that Defendant will continue to fail to protect Sensitive Information, including PII, entrusted to them, as detailed herein.

110. Plaintiff will mail this complaint to the Attorney General within 10 days of filing, pursuant to N.J.S.A. 56:8-20.

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

THIRD CLAIM FOR RELIEF

Violation of Florida Deceptive and Unfair Trade Practices Act,
Fla. Stat. § 501.202, *et seq.*
(Against Defendants Quest and Optum360 on behalf of
Plaintiff Benadom and the Florida Subclass)

112. Plaintiff incorporate paragraphs 1–67 as if fully set forth herein.

113. The Florida Deceptive and Unfair Trade Practices Act declares that "Unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." Fla. Stat. § 501.204(1).

114. At all relevant times material hereto, Defendants conducted trade or commerce, or furnished services, in the State of Florida.

115. Defendants, while conducting trade or commerce or furnishing services in the State of Florida, engaged in deceptive acts and practices in violation of Fla. Stat. § 501.204, because:

a. Defendants failed to enact adequate privacy and security measures to protect the Class Members' Sensitive Information from unauthorized disclosure, release, data breach or theft;

b. Defendants failed to take proper action to address known security risks;

c. Defendants made false or misleading misrepresentations that they would maintain adequate data privacy and security practices and procedures to safeguard the Sensitive Information from unauthorized disclosure, release, data breach or theft;

d. Defendants failed to disclose, omitted, actively concealed the material fact of the inadequacy of their data security or the true characteristics and quality of their data security; and

e. Defendants made false or misleading misrepresentations that that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Sensitive Information.

116. The above listed acts were unfair or deceptive because they were likely to mislead a reasonable consumer acting reasonably under the circumstances, and such acts were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class members.

117. As set out above, since only Defendants knew (or should have known) that they were not complying with their own data security representations and obligations, there was no way for members of the public, including Plaintiff and members of the Classes, to avoid the injury caused by Defendants' conduct. Defendants' failure to use adequate data security practice and failure to live up to their data security representations and obligations did not create any countervailing benefits.

118. Plaintiff and the proposed class members reasonably expected that Defendants would protect their Sensitive Information provide truthful statements regarding their privacy policies.

119. Defendants engaged in omission of material facts, deception, active concealment, and misrepresentation with the intent that consumers would rely on the same when providing Sensitive Information to Defendants.

120. Defendants' failure to disclose their actual (and substandard) security practices substantially injured the public because it caused millions of consumers to enter into transactions they otherwise would not have, and because it compromised the integrity of Plaintiff's and the Classes Sensitive Information. Further, Defendants' use of substandard security did not create any benefits sufficient to outweigh the harm it caused.

121. Defendants' unfair or deceptive acts or practices and general course of conduct is injurious to the public interest, and such acts are ongoing and/or have a substantial likelihood of being repeated inasmuch as the long-lasting harmful effects of their misconduct may last for years (e.g., affected individuals could experience identity theft for years). As such, Defendants' violations present a continuing risk to Plaintiff and Class Members, as well as to the general public.

122. As a result of Defendants' conduct, Plaintiff and members of the Classes have suffered actual damages, including the lost value of their Sensitive Information; the lost value of their personal data and lost property in the form of their breached and compromised Sensitive Information (which is of great value to third parties); ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

123. Plaintiff seeks relief under Fla. Stat. § 501.211, including but not limited to actual damages, in an amount to be proven at trial, and reasonable attorney's fees and costs.

124. Plaintiff also seeks to enjoin Defendants from their unfair and deceptive acts and practices described above. Each Class member will be irreparably harmed unless the Court enjoins Defendants' unlawful, deceptive actions in that Defendants will continue to fail to protect Sensitive Information entrusted them, as detailed herein.

125. In the event that Florida 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 each of the fifty states.

VII. REQUEST FOR RELIEF

Plaintiff, on behalf of himself and the Classes, respectfully request that this Court enter an Order:

1. Certifying this case as a class action on behalf of Plaintiff and the Classes defined above, appointing Plaintiff as Class Representatives of the Classes, and appointing Plaintiff's counsel to represent the Classes;

2. Awarding Plaintiff and Class Members appropriate relief, including actual and statutory damages;

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

4. Awarding Plaintiff and the Classes their reasonable litigation expenses and attorneys' fees;

5. Awarding Plaintiff and the Classes pre- and post-judgment interest, to the extent allowable by law;

6. Permitting Plaintiff and the Classes to amend their pleadings to conform to the evidence produced at trial; and

7. Awarding such other and further relief as equity and justice may require.

VIII. JURY DEMAND

Plaintiff requests a trial by jury.

LITE DEPALMA GREENBERG LLC

Dated: June 20, 2019

/s/ Bruce D. Greenberg

Bruce D. Greenberg
570 Broad Street, Suite 1201
Newark, NJ 07102
Telephone: (973) 877-3820
Facsimile: (973) 623-0858
bgreenberg@litedepalma.com

HAUSFELD LLP
James Pizzirusso*
1700 K. Street NW, Suite 650
Washington, DC 20006
Tel: 202.540.7200
Fax: 202.540.7201
jpizzirusso@hausfeld.com

TOUSLEY BRAIN STEPHENS, PLLC
Kim D. Stephens*
Jason T. Dennett*
Cecily C. Shiel*
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992
kstephens@tousley.com
jdennett@tousley.com
cshiel@tousley.com

PEARSON, SIMON & WARSHAW, LLP
Daniel L. Warshaw*
15165 Ventura Boulevard, Suite 400
Sherman Oaks, California 91403
Telephone: (818) 788 8300
Facsimile: (818) 788 8104
dwarshaw@pswlaw.com

PEARSON, SIMON & WARSHAW, LLP
Melissa S. Weiner*
Joseph C. Bourne *
800 LaSalle Avenue, Suite 2150
Minneapolis, Minnesota 55402
Telephone: (612) 389-0600
Facsimile: (612) 389-0610
mweiner@pswlaw.com
jbourne@pswlaw.com

Attorneys for Plaintiff and the Proposed Class

**Pro hac vice* applications forthcoming

LOCAL CIVIL RULE 11.2 CERTIFICATION

Pursuant to Local Civil Rule 11.2, I hereby certify that the matter in controversy is related to the following civil action:

- *Vieyra v. Quest Diagnostics, Inc. et al.*, 2:19-13396 (D.N.J.) (MCA)(SCM)
- *Fernandez v. American Medical Collection Agency, Inc. et al.*, 2:19-13398 (D.N.J.) (MCA)(SCM)
- *Carbonneau v. Quest Diagnostics Incorporated et al.*, 2:19-13472 (D.N.J.) (MCA)(SCM)
- *Meisel et al. v. American Medical Collection Agency, Inc. et al.*, 2:19-13484 (D.N.J.) (MCA)(SCM)
- *Rahill v. Quest Diagnostics et al.*, 2:19-cv-13510 (D.N.J.) (WHW)(CLW)

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

Dated: June 20, 2019

LITE DEPALMA GREENBERG LLC

/s/ Bruce D. Greenberg
Bruce D. Greenberg
570 Broad Street, Suite 1201
Newark, NJ 07102
Telephone: (973) 877-3820
Facsimile: (973) 623-0858
bgreenberg@litedepalma.com

HAUSFELD LLP
James Pizzirusso*
1700 K. Street NW, Suite 650
Washington, DC 20006
Tel: 202.540.7200
Fax: 202.540.7201
jpizzirusso@hausfeld.com

TOUSLEY BRAIN STEPHENS, PLLC
Kim D. Stephens*
Jason T. Dennett*
Cecily C. Shiel*
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992

kstephens@tousley.com
jdennett@tousley.com
cshiel@tousley.com

PEARSON, SIMON & WARSHAW, LLP
Daniel L. Warshaw*
15165 Ventura Boulevard, Suite 400
Sherman Oaks, California 91403
Telephone: (818) 788 8300
Facsimile: (818) 788 8104
dwarshaw@pswlaw.com

PEARSON, SIMON & WARSHAW, LLP
Melissa S. Weiner*
Joseph C. Bourne *
800 LaSalle Avenue, Suite 2150
Minneapolis, Minnesota 55402
Telephone: (612) 389-0600
Facsimile: (612) 389-0610
mweiner@pswlaw.com
jbourne@pswlaw.com

Attorneys for Plaintiff and the Proposed Class

**Pro hac vice* applications forthcoming