BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
THOMAS J. O'REARDON II (247952)
JENNIFER L. MACPHERSON (202021)
501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
toreardon@bholaw.com
jmacpherson@bholaw.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

[redacted], individually and on behalf of all others similarly situated,

Plaintiff,

v.

QUEST DIAGNOSTICS INCORPORATED d/b/a QUEST DIAGNOSTICS INCORPORATED OF NEVADA; OPTUM360 SERVICES, INC.; and AMERICAN MEDICAL COLLECTION AGENCY a/k/a RETRIEVAL-MASTERS CREDITORS BUREAU, INC.,

Defendants.

Case No. 2:19-cv-05071

CLASS ACTION

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff [redacted] ("Plaintiff"), individually and on behalf of the general public and all others similarly situated (the "Class members"), by and through his attorneys, upon personal knowledge as to facts pertaining to himself and on information and belief as to all other matters, brings this action against Defendants Quest Diagnostics Incorporated ("Quest"); Optum360 Services, Inc. ("Optum 360"); and American Medical Collection Agency ("AMCA") (collectively, "Defendants"), and respectfully state the following:

NATURE OF THE CASE

1. Quest Diagnostics is a leading provider of medical diagnostic testing, information and services. Its services range from routine blood testing to complex, gene-based and molecular testing. With one of the largest clinical laboratory testing networks in the United States, Quest annually serves one in three adult Americans and half the physicians and hospitals in the United States. Quest Diagnostics' billing is conducted through its partnership with Optum360, who outsources collections to AMCA.

2. On June 3, 2019, Quest Diagnostics revealed that personally identifiably information ("PII") and protected health information ("PHI") (collectively, "PII/PHI") of nearly 12 million of its patients had been accessed by unauthorized parties due to the negligent data security of AMCA, its third-party billing collections firm (the "Data Breach"). The PII/PHI accessed included, but was not limited to, Plaintiff's and Class members' personal information (including Social Security Numbers), financial information (credit card numbers and bank account information), and personal medical information.

3. AMCA knew or should have known about the Data Breach as early as March 1, 2019 but waited over two months to disclose it to Quest Diagnostics and Optum360 (on May 14, 2019) who waited another twenty days to inform Plaintiff and Class members (on June 3, 2019).

4. At least some of Plaintiff and Class member information already appears up for sale on the dark web. In February 2019, Gemini Advisory, a New York-based company that monitors underground markets trafficking in breached data, discovered PII/PHI from AMCA being sold on the dark web.

5. Defendants had a legal duty to protect the PII/PHI of Plaintiff and Class members. For instance, California's Confidentiality of Medical Information Act ("CMIA"), Civil Code §§ 56, *et seq*., protects the confidentiality of individually identifiable medical information obtained by a health care provider. Defendants breached the CMIA by failing to adequately secure Plaintiff's and Class members' PII/PHI.

6. On top of their legal duty, Defendants promised Plaintiff and Class members their PII/PHI was protected. Quest Diagnostics tells patients that it is "committed to protecting the privacy of your identifiable health information." Optum360 similarly "recognize[s] that the privacy of your personal information is important," promising to "safeguard the information of those we serve."

7. Defendants' wrongful actions, inaction, and omissions directly and proximately caused the Data Breach. Specifically, Defendants failed to maintain reasonable and/or adequate security measures to protect Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure, apparently lacking, at a minimum: (1) reasonable and adequate security measures designed to prevent this attack even though Defendants knew or should have known that it was a prized target for hackers; and (2) reasonable and adequate security protocols to promptly detect the unauthorized intrusion into and removal of PII/PHI from its database pertaining to nearly 12 million Data Breach victims.

8. Defendants' failure to secure Plaintiff's and Class members' PII/PHI has resulted in ongoing harm to Plaintiff and Class members who will continue to experience data insecurity for the indefinite future and remain at serious risk of identity theft and medical fraud.

9. Accordingly, Plaintiff, on behalf of himself and all others similarly situated, seeks redress from Defendants for, *inter alia*, violations of California's Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq*., California's Customer Records Act, Civil Code §§ 1798.80, *et seq*. ("CRA"), California's Unfair Competition Law ("UCL"), Bus. & Prof. Code §§ 17200, *et seq*., and common law. Plaintiff, on behalf of himself and all others similarly situated, seeks (i) actual and other economic damages, consequential damages, nominal damages, and/or statutory damages, (ii) punitive damages, and (iii) attorneys' fees, litigation expenses and costs of suit.

PARTIES

10. [redacted] For the past year, Plaintiff has obtained laboratory services from Quest Diagnostics at several locations in [redacted] California. During these visits Plaintiff provided Quest with confidential PII/PHI that was shared with the other Defendants. At least one of Plaintiff's bills for services provided by Quest Diagnostics was sent to AMCA for collections.

11. Plaintiff believed, at the time of using Quest Diagnostics, that it would maintain and ensure the privacy and security of his PII/PHI. Part of the money paid to Quest was for adequate data security. Plaintiff would not have used Quest had he known that it would expose, or allow to be exposed, his PII/PHI, making it available to unauthorized parties. As a result of Defendants' wrongful actions, inaction and/or omissions, Plaintiff has suffered (and will continue to suffer) economic damages and injury and harm, including: (i) substantial risk for identity theft[1] and medical fraud[2];

[1] According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia*, credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services, including medical services).

[2] Medical fraud (or medical identity theft) occurs when a data thief uses a

(ii) invasion of privacy; (iii) breach of the confidentiality of his PII/PHI; (iv) deprivation of the value of his PII/PHI, for which there is a well-established national and international market; and/or (v) the financial and/or temporal cost of monitoring his credit, monitoring his financial accounts and medical records, among others, and mitigating his damages – for which he is entitled to compensation.

12. Defendant Quest Diagnostics Incorporated is a Nevada corporation that does business in California as Quest Diagnostics Incorporated of Nevada. The principal place of business for Quest Diagnostics Incorporated is Secaucus, New Jersey. Quest Diagnostics is a leading provider of diagnostic testing, information and services. Its services range from routine blood testing to complex, gene-based and molecular testing. With one of the largest clinical laboratory testing networks in the United States, Quest annually serves one in three adult Americans and half the physicians and hospitals in the United States.

13. Defendant Optum360 Services, Inc. is a Delaware corporation with its principal place of business in Eden Prairie, Minnesota. Optum is a leading information and technology-enabled health services business and a leader in revenue management solutions for health care providers. In September 2016, Quest Diagnostics and Optum partnered together. Through this partnership Quest Diagnostics' revenue services operations became part of Optum360. These operations, including approximately 2,400 Quest employees, moved to Optum360 and continued to support Quest customers. One goal of the partnership was to increase the use of diagnostic information services, such as data analytics, population health insights and connectivity solutions, to help improve health care effectiveness and manage costs for

---

victim's name or health insurance numbers to see a doctor, get prescription drugs, file claims with insurance providers, or obtain other medical care. *See* http://www.consumer.ftc.gov/articles/0171-medical-identity-theft. If the thief's health information is mixed with the victim's information, the victim's medical treatment, insurance and payment records, and credit report may be affected. *Id.*

health plans and care providers.

14. Defendant American Medical Collection Agency, which also does business as Retrieval-Masters Creditors Bureau, Inc., is a New York corporation with its principal place of business in Elmsford, New York. AMCA describes itself as the leading recovery agency for patient collections servicing laboratories, hospitals, physician groups, billing services and medical providers across the country. AMCA provides billing collections services to Optum360, which in turn is a Quest contractor.

VENUE AND JURISDICTION

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 Class members, the amount in controversy exceeds $5 million exclusive of interest and costs, and many members of the Class are citizens of states different from Defendants.

16. This Court has personal jurisdiction over Quest Diagnostics Incorporated because Quest is authorized to conduct business in California and does, in fact, conduct business in California. Upon information and belief Quest has over 400 laboratories throughout California. As such, Quest has sufficient minimum contacts with the state to render exercise of jurisdiction by this Court in compliance with traditional notions of fair play and substantial justice.

17. This Court also has personal jurisdiction over Optum360 Services, Inc. because Optum360 is authorized to conduct business in California and does, in fact, conduct business in California. Optum360 has offices in California. As such, Optum360 has sufficient minimum contacts with the state to render exercise of jurisdiction by this Court in compliance with traditional notions of fair play and substantial justice.

18. This Court has personal jurisdiction over American Medical Collection Agency doing business as Retrieval-Masters Creditors Bureau, Inc. because Retrieval-Masters Creditors Bureau, Inc. is authorized to and conducts substantial

business in California and has a principal office in California located at 1215 West Imperial Highway, Suite 215, Brea, California 92621. AMCA therefore has sufficient minimum contacts with the state to render exercise of jurisdiction by this Court in compliance with traditional notions of fair play and substantial justice.

19. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391 because Defendants regularly conduct business in this district, unlawful acts or omissions are alleged to have occurred in this district, and Defendants are subject to personal jurisdiction in this district because they have availed themselves of the laws and markets within this district.

FACTUAL ALLEGATIONS

PII/PHI Is a Valuable Property Right

20. PII/PHI is a valuable property right.[3] In a Federal Trade Commission ("FCC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[4]

21. The value of PII/PHI as a commodity is measurable.[5] "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level

---

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

[4] Federal Trade Commission, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), *available at* https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

[5] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market* (April 28, 2014), *available at*

comparable to the value of traditional financial assets."[6] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market" for several years.

22. Companies recognize PII/PHI as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[7]

23. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

24. PHI is particularly valuable. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[8] According to a report released by the Federal Bureau of

---

http://www.medscape.com/viewarticle/824192.

[6] *See* Soma, *Corporate Privacy Trend*, *supra*.

[7] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

[8] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market* (July 16, 2013), *available at* https://www.scmagazine.com/home/security-news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/.

Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen social security or credit card number.[9]

25. Recognizing the high value that consumers place on their PII/PHI, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII/PHI.[10] This business has created a new market for the sale and purchase of this valuable data.[11]

26. Consumers place a high value not only on their PII/PHI, but also on the *privacy* of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[12]

27. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per

---

[9] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014) *available at* https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[10] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/18unboxed.html.

[11] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576160764037920 27.

[12] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1#page_scan_tab_contents.

website.[13]

28. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

29. Theft of PII/PHI is serious. The United States Government Accountability Office noted in a June, 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[14] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

30. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[15]

31. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[16]

---

[13] II–Horn, Hann et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

[14] *See* http:///www.gao.gov/new.items/d07737.pdf.

[15] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

[16] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. 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

According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receive bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[17]

32. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[18] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[19] "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[20]

33. A report published by the World Privacy Form and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[17] *See* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[18] Pam Dixon, et al., *The Geography of Medical Identity Theft* (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf.

[19] *See* https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (FBI, April 8, 2014).

[20] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

34. A person whose PII/PHI has been compromised may not see any signs of identity theft for years. According to the GAO Report:

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

35. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[21].

36. It is within this context that Plaintiff and almost 12 million patients must now live with the knowledge that their PII/PHI is forever in cyberspace and

[21] *See* https://blog.linkedin.com/2016/05/18/protecting-our-members.

was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

The Data Breach

37. Plaintiff and Class members are customers who paid money for and provided their PII/PHI to Quest Diagnostics in exchange for diagnostic and medical services. Quest Diagnostics provided Plaintiff and Class members' PII/PHI to Optum360 who in turn provided that information to AMCA for billing and collection purposes.

38. For more than six months, from August 1, 2018 to March 30, 2019, unauthorized parties accessed the AMCA system containing the PII/PHI of nearly 12 million customers of Quest Diagnostics, including Plaintiff and Class members. This information included personal information (e.g., Social Security Numbers), financial information (credit card numbers and bank account information), and medical information.

Defendants Failed to Timely Disclose the Data Breach

39. AMCA claims it was alerted to the breach after receiving information from a security compliance firm that works with credit card companies of a possible security compromise.

40. Upon information and belief that firm was Gemini Advisory. Gemini Advisory's Director of Research stated that on March 1, 2019, it tried unsuccessfully to notify AMCA of the Data Breach. Not getting any response from AMCA, Gemini contacted federal law enforcement, who reportedly followed up by contacting AMCA.

41. AMCA then waited until May 14, 2019, over two months, to inform Quest Diagnostics and Optum360 of the Data Breach. Quest and Optum360 waited another two weeks to inform Plaintiff and Class members, only doing so through a June 3, 2019 SEC filing.

42. AMCA has not notified Plaintiff and Class members about the Data Breach. Instead it made the following statement through an outside PR firm: "We are investigating a data incident involving an unauthorized user accessing the American Medical Collection Agency system[.]"

43. Upon information and belief no Defendant has individually noticed any of the almost 12 million Plaintiff and Class Members affected by the Data Breach. Further, no Defendant has offered any form of credit monitoring or other protective measures to help protect Plaintiff and Class members from identity theft and/or medical fraud.

The Breached PII/PHI Is Already Being Sold on the Dark Web

44. Defendants' failure to safeguard Plaintiff and Class members PII/PHI, failure to timely notify Plaintiff and Class members of the Data Breach, and failure to offer any protective measures to assist Plaintiff and Class members in avoiding identity theft and/or medical fraud has serious consequences.

45. On May 10, 2019, Gemini Advisory confirmed that at the end of February its analysts identified a Card Not Present (CNP) database that had been posted for sale in a dark web market. The offering had been described as "USA|DOB|SSN," and because CNP data is rarely sold with associated date of birth and Social Security numbers, Gemini Advisory analysts suspected a compromise in an online portal that would collect these types of data as part of a transaction.

46. Through further analysis, Gemini analysts identified several top affected banks that primarily focus on Health Savings Accounts (HSAs), Health Reimbursement Accounts (HRAs), Flexible Spending Accounts (FSAs), and Medicare Medical Savings Accounts (MSAs). These various medical accounts are used to pay health insurance deductibles, dental and vision care, and any other qualifying medical expenses. Analysis revealed the information was likely stolen from the online portal of AMCA.

47. In a statement to DataBreaches.net, Gemini Advisory's Director of Research, Stas Alforov, explained that: "[o]n February 28, 2019, Gemini Advisory identified a large number of compromised payment cards while monitoring dark web marketplaces. Almost 15% of these records included additional personally identifiable information (PII), such as dates of birth (DOBs), Social Security numbers (SSNs), and physical addresses. A thorough analysis indicated that the information was likely stolen from the online portal of the American Medical Collection Agency (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."

48. Gemini Advisory's Director of Research explained why this is so serious:

> Health Savings Accounts (HSAs) are often tied to specialized debit cards that are used to make medical-based payments but can also be used for regular purchases at the cost of a severe tax penalty.
>
> Account holders often only periodically use HSAs due to the incentives for accumulating funds that can later be withdrawn without any penalties during retirement, meaning that they are likely not as closely monitored for any daily unauthorized activities. Thus, they make easier targets for criminal actors who attempt to monetize the compromised data from medical breaches such as AMCA's.
>
> We are often encouraged to — and many of us do — routinely and regularly check our bank statements for unusual activity or check our credit card statements for signs of misuse. But if you have an account linked to a debit or credit card that you do not use except for paying medical bills in an emergency or it is your savings account for your future care, then criminals could be draining your account and you may not find out in time to report the theft to your bank. And without timely reporting, your bank might not restore your funds or cover your losses.[22]

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

Defendants Promised to Protect Plaintiff and Class Members' PII/PHI

49. Quest Diagnostics promised to maintain the security and privacy of Plaintiff's and Class members' personal information. In its Notice of Privacy Practices, Quest Diagnostics promised its customers that it was "committed to protecting the privacy of your identifiable health information."

50. Quest Diagnostics also acknowledges the following:

> 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. We are required to notify affected individuals in the event of a breach involving unsecured protected health information. PHI is stored electronically and is subject to electronic disclosure. This Notice does not apply to non-diagnostic services that we perform such as certain drugs of abuse testing services and clinical trials testing services.

51. Quest Diagnostics also ensures its customers that it will only use their PII/PHI for certain limited purposes, such as "for treatment, payment, or healthcare operations purposes and for other purposes permitted or required by law." Quest Diagnostics states:

> We need your written authorization to use or disclose your health information for any purpose not covered by one of the categories below. Subject to compliance with limited exceptions, we will not use or disclose psychotherapy notes, use or disclose your PHI for marketing purposes or sell your PHI, unless you have signed an authorization. You may revoke any authorization you sign at any time. If you revoke your authorization, we will no longer use or disclose your health information for the reasons stated in your authorization except to the extent we have already taken action based on your authorization.

52. While Plaintiff and Class members were likely unaware that Quest Diagnostics had shared their PII/PHI with AMCA or Optum360 these companies provided similar assurances of data security.

53. Optum360 claims that "[p]rotecting our consumer and customer information is very important. We safeguard the information of those we serve. Optum handles and safeguards personal information, and we understand the information we hold represents real people and life events." It also promises that "Optum Privacy is dedicated to the responsible and compliant collection, use, maintenance and disclosure of information for the individuals and customers we serve. The Optum Privacy Program is designed to protect information and to comply with applicable privacy rules and regulations."

54. With respect to Social Security Numbers Optum360 promises customers that it will "secure the confidentiality of SSNs through various means, including physical, technical, and administrative safeguards that are designed to protect against unauthorized access. It is our policy to limit access to SSNs to that which is lawful, and to prohibit unlawful disclosure of SSNs."

55. AMCA tells customers it is "compliant with all Federal and State Laws." In a statement issued after the Data Breach, AMCA commented that it "remain[s] committed to our system's security, data privacy, and the protection of personal information."

56. By failing to protect Plaintiff and Class member's PII/PHI, and by allowing the Data Breach to occur, Defendants broke their privacy promises.

57. To date, Defendants have not yet provided a Notice of Data Breach and have not adequately explained how the Data Breach occurred and why it took a third party to inform it of the Data Breach.

Defendants Were Legally Obligated to Protect Patients' PHI

58. Quest Diagnostics recognizes that it "is required by law to maintain the privacy of [] [patient] PHI." Those laws include but are not limited to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), California's Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56, *et seq.*, and

California's Customer Records Act ("CRA"), Cal. Civ. Code §§ 1798.80, *et seq*., among others.

59. As a healthcare provider, Defendants are subject to the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "Privacy and Security Rules").

60. The HIPAA Privacy and Security Rules establish a national set of standards for the protection of "individually identifiable health information" that is held or transmitted by a health care provider, which HIPAA refers to as "protected health information." Pursuant to HIPAA, Defendants must maintain (and review and modify as needed) reasonable and appropriate administrative, technical, and physical standards and safeguards for protecting PHI (e.g., 45 C.F.R. §§ 164.306(a), (e); 164.312(a), (d), (e); 164.316(a), (b).) Under the HIPAA Privacy Rule, Defendants may not use or disclose PHI or confidential medical information except as expressly permitted, 45 CFR 164.502(a).

61. Under HIPAA Defendants must implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems (e.g., 45 CFR §§ 164.308(a), 164.306(d), 164.312).[23]

62. California's Confidentiality of Medical Information Act prohibits healthcare providers and contractors from disclosing a patient's confidential medical information without prior authorization. Cal. Civ. Code § 56.10(a). The CMIA states

[23] *See* Office for Civil Rights, *Guidance on Risk Analysis Requirements under the HIPAA Security Rule* (July 14, 2010) *available at* https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

that "a provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or enrollee or subscriber of a health care service plan without first obtaining an authorization except as provided in subdivision (b) or (c)."

63. California's Customer Records Act requires a business to notify without unreasonable delay any California resident whose unencrypted personal information, including health data, personal identifiers, credit cards, insurance details, and other personal information, was acquired, or reasonably believed to have been acquired, by an unauthorized person. Cal. Civ. Code § 1798.82(a).

64. In addition to their obligations under federal and state laws and regulations, Defendants owed a common law duty to Plaintiff and Class members to protect PII/PHI entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

65. As a direct and proximate result of Defendants' reckless and negligent actions, inaction, and omissions, the resulting Data Breach, the unauthorized release and disclosure of Plaintiff's and Class members' PII/PHI, and Defendants' failure to properly and timely notify Plaintiff and Class members, Plaintiff and Class members have experienced, will continue to experience, and will face an increased risk of identity and medical theft and fraud and/or other unauthorized uses of personal information for which they have expended and/or will expend substantial money and time to prevent, detect, contest, and repair.

Defendants Knew or Should Have Known PII/PHI Are High Risk Targets

66. Defendants knew or should have known that PII, and in particular, PHI, are high risk targets for identity thieves. In 2014, the FBI informed that "[c]yber actors will likely increase cyber intrusions against healthcare systems" and warned that the

"healthcare industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures[.]"[24]

67. The Identity Theft Resource Center reported that the Medical/Healthcare sector had the second largest number of breaches in 2018 and the highest rate of exposure per breach. According to the ITRC this sector suffered 363 data breaches exposing over 9 million records in 2018.[25] These included Blue Cross Blue Shield of Michigan (15K records exposed), Atrium Health (over 2M records exposed), UnityPoint Health (over 1M records), LifeBridge Health (over 500K), FastHealth Corporation (over 600K records), among others.

68. As such, Defendants were aware that PHI is at high risk of theft, and consequently should have but did not take appropriate and standard measures to protect Plaintiff's and Class member's PII/PHI against cyber-security attacks that Defendants should have anticipated and guarded against.

CLASS DEFINITION AND ALLEGATIONS

69. Plaintiff brings all claims as class claims under Federal Rule of Civil Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4).

70. Plaintiff brings all claims on behalf of a proposed Nationwide Class and California Sub-Class, defined as follows:

> Nationwide Class: All persons in the United States whose PII/PHI was accessed by and disclosed to unauthorized persons in the Data Breach.
>
> California Sub-Class: All persons in the State of California whose PII/PHI was accessed by and disclosed to unauthorized persons in the Data Breach.

[24] *See* https://publicintelligence.net/fbi-health-care-cyber-intrusions/ (FBI, April 8, 2014).

[25] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, *available at* https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

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

72. **Numerosity.** While the exact number of Class and Sub-Class members is unknown, Defendants have admitted the PII/PHI, including personal information (e.g., Social Security Numbers), financial information (credit card numbers and bank account information), and medical information of nearly 12 million Plaintiff and Class members was compromised in the Data Breach. Plaintiff therefore believes that the Classes are so numerous that joinder of all members is impractical.

73. **Typicality.** Plaintiff's claims are typical of the claims of the Class and Sub-Class. Plaintiff, like all proposed members of each Class, had his PII/PHI compromised in the Data Breach. Plaintiff and members of each Class were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class and Sub-Class members.

74. **Commonality.** Common questions of law and fact exist as to all Class and Sub-Class members and predominate over any individual questions. Such common questions include, but are not limited to:

(a) Whether Defendants engaged in the alleged wrongful, unlawful, unfair or fraudulent business acts or practices;

(b) Whether Defendants owed a duty to Plaintiff and each Class and Sub-Class member to adequately protect their PII/PHI;

(c) Whether Defendants breached their duties to protect the PII/PHI of Plaintiff and each Class and Sub-Class member;

(d) Whether Defendants knew or should have known that AMCA's data security systems, policies, procedures, and practices were vulnerable;

(e) Whether Plaintiff and each Class and Sub-Class member suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity/medical theft and fraud, and loss of value of PII/PHI;

(f) Whether Defendants' conduct violated the laws alleged;

(g) Whether Plaintiff and each Class and Sub-Class member are entitled to restitution, disgorgement, and other equitable relief; and

(h) Whether Plaintiff and each Class and Sub-Class member are entitled to recover actual damages, statutory damages, and punitive damages.

75. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the Class and Sub-Class members. Plaintiff is an adequate representative of the Class and Sub-Class in that he has no interests adverse to or that conflict with the Classes Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

76. **Superiority.** A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class and Sub-Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class and Sub-Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class and Sub-Class may be relatively small. Even if the Class and Sub-Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

///

FIRST CAUSE OF ACTION

Violation of the California Confidentiality of Medical Information Act (Civil Code §§ 56, *et seq.*)

(Plaintiff and All Classes Against Quest Diagnostics and Optum360)

77. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

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

79. Quest Diagnostics and Optum360 are "contractor[s]" within the meaning of Civil Code § 56.05(d) and/or "provider[s] of health care" within the meaning of Civil Code § 56.06 and maintained and continue to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Defendants, within the meaning of Civil Code § 56.05(k).

80. Plaintiff and all members of the Classes are "patients" of Defendants within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiff and the Classes fear that disclosure of their medical information could subject them to harassment or abuse.

81. Plaintiff and members of the Classes, as patients of Defendants, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendants' computer network at the time of the breach.

82. Defendants, through inadequate security, allowed an unauthorized third party to gain access to Plaintiff's and each Class members' medical information, without the prior written authorization of Plaintiff and the Classes, as required by Civil Code § 56.10 of the CMIA.

83. Defendants violated Civil Code § 56.101 of the CMIA through their failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the Classes.

84. As a result of Defendants' above-described conduct, Plaintiff and the Classes have suffered damages from the unauthorized release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101.

85. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and members of each Class have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia,* (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the California CMIA and CRA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

86. Plaintiff, individually and for each member of the Classes, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiff and each Class member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

///

///

///

SECOND CAUSE OF ACTION

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

(Plaintiff and California Sub-Class Against All Defendants)

87. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

88. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted the Customer Records Act, Civil Code § 1798.81.5, which requires that any business that "owns licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

89. Defendants are "businesses" within the meaning of Civil Code § 1798.80(a).

90. The information Defendants "own" or "license" or "maintain" is the kind defined by Civil Code § 1798.81.5(a)(2).

91. As described above, Defendants failed to implement and maintain reasonable security procedures and practices to protect the Plaintiff's and California Sub-Class members' "personal information" as that term is defined in Civil Code § 1798.80(e) and § 1798.81.5(d), which resulted in the Data Breach.

92. Defendants also unreasonably delayed and failed to disclose the Data Breach to Plaintiff and California Sub-Class members in the most expedient time possible and without unreasonable delay when they knew, or reasonably believed, Plaintiff's and California Sub-Class members' personal information had been wrongfully disclosed to an unauthorized person or persons.

93. Under California Civil Code § 1798.82, any person or business that "owns or licenses computerized data that includes personal information" of California

residents must promptly and "in the most expedient time possible and without unreasonable delay" disclose any Data Breach involving such retained data.

94. As a result of Defendants' violations of Civil Code §§ 1798.81.5 and 1798.82, Plaintiff and members of the California Sub-Class have incurred and will incur damages, including but not necessarily limited to: (1) the loss of the opportunity to control how their personal information (PII/PHI) is used; (2) the compromise, publication, and/or theft of their personal information; (3) out-of-pocket costs associated with the prevention, detection, insurance, and recovery from identity and medical theft and fraud, and unauthorized use of financial and medical accounts; (4) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and medical fraud and data misuse; (5) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (6) unauthorized use of compromised personal information to open new financial and/or health care or medical accounts; (7) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (8) the continued risk to their personal information, which remain in Defendants' possession and are subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the personal information in their possession; and (9) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the personal information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the California Sub-Class members.

95. Plaintiff seeks all remedies available under Civil Code § 1798.84, including actual and statutory damages, equitable relief, and reasonable attorneys' fees.

96. Plaintiff is also entitled to injunctive relief under Civil Code § 1798.84(e).

THIRD CAUSE OF ACTION

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

(Plaintiff and All Classes Against All Defendants)

97. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

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

99. In the course of conducting their businesses, Defendants committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class members' PII/PHI, and violating the statutory and common law alleged herein in the process, including, *inter alia*, California's Confidentiality of Medical Information Act (Civ. Code §§ 56, *et seq*.), California's Customer Records Act (Civ. Code §§ 1798.80, *et seq*.), California's Insurance Information and Privacy Protection Act (Cal. Ins. Code §§ 791, *et seq*.), HIPAA (42 U.S.C. §§ 1302d, *et seq*.), the Gramm-Leach-Bliley Act (15

U.S.C. §§ 6801, *et seq.*), and Article I, Section 1 of the California Constitution (California's constitutional right to privacy). Plaintiff and Class members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

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

101. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendants' wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendants' practices are also contrary to legislatively declared and public policies that seek to protect PII/PHI and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as California's Confidentiality of Medical Information Act (Civ. Code § §56, *et seq.*), California's Customer Records Act (Civ. Code §§ 1798.80, *et seq.*), California's Insurance Information and Privacy Protection Act (Cal. Ins. Code §§ 791, *et seq.*), HIPAA (42 U.S.C. §§ 1302d, *et seq.*), the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801, *et seq.*), and Article I, Section 1 of the California Constitution (California's constitutional right to privacy). The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendants' legitimate business interests other than engaging in the above-described wrongful conduct.

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

103. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the UCL, Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity and medical theft and identity and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the California CMIA and CRA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

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

///

///

FOURTH CAUSE OF ACTION

Negligence

(Plaintiff and All Classes Against All Defendants)

105. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

106. Defendants had (and continue to have) a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII/PHI.

107. Defendants also had (and continue to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated (such as in the storage and protection of private, non-public PII/PHI within their possession, custody and control). Such affirmative duties also are expressly imposed upon Defendants from other sources enumerated herein.

108. Defendants' duties arise from, *inter alia*, California's Confidentiality of Medical Information Act (Civ. Code §§ 56, *et seq*.), California's Customer Records Act (Civ. Code §§ 1798.80, *et seq*.), California's Insurance Information and Privacy Protection Act (Cal. Ins. Code §§ 791, *et seq*.), HIPAA (42 U.S.C. §§ 1302d, *et seq*.), the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801, *et seq*.), Article I, Section 1 of the California Constitution (California's constitutional right to privacy), and the UCL, (Cal. Bus. & Prof. Code §§ 17200, *et seq*.).

109. The above-outlined standards and duties exist for the express purpose of protecting Plaintiff, Class members and their PII/PHI.

110. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it – including Plaintiff's and Class members' PII/PHI.

111. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI for no lawful purpose.

112. Defendants, by and through their above negligent or grossly negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached their duties to Plaintiff and Class members by, among other things, failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI within their possession, custody and control. Defendants, by and through their above negligent or grossly actions, inactions, omissions, and want of ordinary care, further breached their duties to Plaintiff and Class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their PII/PHI.

113. But for Defendants' negligent or grossly negligent breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been released, disclosed, and disseminated – without their authorization – and compromised.

114. Plaintiff's and Class members' PII/PHI was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendants' failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Class members' PII/PHI.

115. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach constitute negligence, gross negligence, and negligence *per se* under California common law.

116. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity and medical theft, and identity and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the California CMIA and CRA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

FIFTH CAUSE OF ACTION

Invasion of Privacy

(Plaintiff and All Classes Against All Defendants)

117. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

118. Plaintiff and Class members have a legally protected privacy interest in their PII/PHI that Defendants required them to provide and allow them to store.

119. Plaintiff and Class members reasonably expected that their PII/PHI would be protected and secured from unauthorized parties, would not be disclosed to any unauthorized parties or disclosed for any improper purpose.

120. Defendants unlawfully invaded the privacy rights of Plaintiff and Class members by (a) failing to adequately secure their PII/PHI from disclosure to unauthorized parties for improper purposes; (b) disclosing their PII/PHI to

unauthorized parties in a manner that is highly offensive to a reasonable person; and (c) disclosing their PII/PHI to unauthorized parties without the informed and clear consent of Plaintiff and Class members. This invasion into the privacy interest of Plaintiff and Class members is serious and substantial.

121. In failing to adequately secure Plaintiff's and Class members' PII/PHI, Defendants acted in reckless disregard of their privacy rights. Defendants knew or should have known that their substandard data security measures are highly offensive to a reasonable person in the same position as Plaintiff and Class members.

122. Defendants violated Plaintiff's and Class members' right to privacy under the common law as well as under state and federal law, including, but not limited to, the California Constitution, Article I, Section I.

123. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff's and Class members' PII/PHI has been viewed or is at imminent risk of being viewed, and their reasonable expectations of privacy have been intruded upon and frustrated. Plaintiff and the proposed Class have suffered injury as a result of Defendants' unlawful invasions of privacy and are entitled to appropriate relief.

SIXTH CAUSE OF ACTION

Breach of Contract

(Plaintiff and All Classes Against Quest Diagnostics)

124. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

125. Plaintiff and Class members, upon information and belief entered into express contracts with Quest Diagnostics that included Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathered on its own, from disclosure.

126. Plaintiff and Class members performed their obligations under the contracts when they provided their PII/PHI to Quest Diagnostics for laboratory and diagnostic services and when they paid for the service provided by Defendants.

127. Quest Diagnostics breached its contractual obligations to protect the nonpublic personal information Quest Diagnostics possessed and was entrusted with when the information was accessed by unauthorized persons as part of the Data Breach.

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

SEVENTH CAUSE OF ACTION

Breach of Implied Contract

(Plaintiff and All Classes Against All Defendants)

129. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

130. Defendants provided Plaintiff and Class members with an implied contract to protect and keep private their PII/PHI.

131. Plaintiff and Class members would not have provided their PII/PHI to Defendants or their subsidiaries or contractors, but for Defendants' implied promises to safeguard and protect their information.

132. Plaintiff and Class members performed their obligations under the implied contract when they provided their PII/PHI to Quest Diagnostics for laboratory and diagnostic services and when they paid for the service provided by Defendants.

133. Defendants breached the implied contracts with Plaintiff and Class members by failing to protect and keep private their PII/PHI.

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

EIGHTH CAUSE OF ACTION

Declaratory Relief

(Plaintiff and All Classes Against All Defendants)

135. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

136. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' duties to safeguard and protect Plaintiff's and Class members' PII/PHI. Defendants' PII/PHI security measures were (and continue to be) woefully inadequate. Defendants dispute these contentions and contend that their security measures are appropriate.

137. Plaintiff and Class members continue to suffer damages, other injury or harm as additional identity and medical theft and fraud occurs.

138. Therefore, Plaintiff and Class members request a judicial determination of their rights and duties, and ask the Court to enter a judgment declaring, *inter alia*, (i) Defendants owed (and continue to owe) a legal duty to safeguard and protect Plaintiff's and Class members' confidential and sensitive PII/PHI, and timely notify them about the Data Breach, (ii) Defendants breached (and continue to breach) such legal duties by failing to safeguard and protect Plaintiff's and Class members' PII/PHI, and (iii) Defendants' breach of their legal duties directly and proximately caused the Data Breach, and the resulting damages, injury, or harm suffered by Plaintiff and Class members. A declaration from the Court ordering Defendants to stop their illegal practices is required. Plaintiff and Class members will otherwise continue to suffer harm as alleged above.

NINTH CAUSE OF ACTION

Unjust Enrichment

(Plaintiff and All Classes Against All Defendants)

139. Plaintiff re-alleges and incorporates by reference all paragraphs as if fully set forth herein.

140. Plaintiff and Class members conferred a benefit to Defendants in the form of payment for laboratory and diagnostic services provided by Defendants, part of which was to pay for Defendants to protect and keep private their PII/PHI.

141. Defendants failed to pay for the benefits provided to them by Plaintiff and Class members by failing to protect and keep private the PII/PHI with which Plaintiff and Class members entrusted Defendants.

142. Defendants' failure to pay for the benefits provided to them, i.e., to protect and keep private Plaintiff's and Class members' PII/PHI, was to the detriment of Plaintiff and Class members because it was Plaintiff's and Class members' PII/PHI that was stolen by cyber thieves.

143. As a direct and proximate result of Defendants' failure to pay for the benefits provided to them, Plaintiff and the Class have been harmed and have suffered, and will continue to suffer, damages and injuries, and are entitled to restitution

PRAYER FOR RELIEF

144. **Damages.** As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members suffered (and will continue to suffer) actual, consequential, incidental, and statutory damages and other injury and harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity and medical theft, and identity and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under California's CMIA and CRA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages. Plaintiff and Class members also are entitled to equitable relief, including, without limitation,

disgorgement and restitution. Plaintiff's and Class members' damages were foreseeable by Defendants and exceed the minimum jurisdictional limits of this Court. All conditions precedent to Plaintiff's and Class members' claims have been performed and occurred.

145. **Punitive Damages.** Plaintiff and Class members also are entitled to punitive damages from Defendants, as punishment and to deter such wrongful conduct in the future, pursuant to, *inter alia*, Cal. Civ. Code § 56.35 and California common law. All conditions precedent to Plaintiff's and Class members' claims have been performed and occurred.

146. **Injunctive Relief.** Pursuant to, *inter alia*, California Civil Code § 56.35, California Civil Code § 1798.84(e), California Civil Code § 1798.47, and Cal. Bus. & Prof. Code § 17203, Plaintiff and Class members also are entitled to injunctive relief in multiple forms including, without limitation, (i) credit monitoring, (ii) Internet monitoring, (iii) identity theft insurance, (iv) prohibiting Defendants from continuing their above-described wrongful conduct, (v) requiring Defendants to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to them, (vi) periodic compliance audits by a third party to ensure that Defendants are properly safeguarding and protecting the PII/PHI in their possession, custody and control, and (vii) clear and effective notice to Class members about the serious risks posed by the theft of the PII/PHI and the precise steps that must be taken to protect themselves. All conditions precedent to Plaintiff's and Class members' claims for relief have been performed and occurred.

147. **Attorneys' Fees, Litigation Expenses and Costs.** Plaintiff and Class members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action pursuant to, *inter alia*, California Civil Code § 56.35,

and other authority. All conditions precedent to Plaintiff's and Classes' claims for relief have been performed and occurred.

WHEREFORE, Plaintiff, on behalf of himself and Class members, respectfully request that (i) this action be certified as a class action, (ii) Plaintiff be designated representative of the Class and Sub-Class and (iii) Plaintiff's counsel be appointed as counsel for the Class and Sub-Class. Plaintiff, on behalf of himself and members of the Class and Sub-Class further request that upon final trial or hearing, judgment be awarded against Defendants for:

(i) actual, incidental, consequential, and nominal damages to be determined by the trier of fact;

(ii) statutory damages;

(iii) punitive damages;

(iv) equitable relief, including restitution, disgorgement of all amounts by which Defendants have been unjustly enriched;

(v) pre- and post-judgment interest at the highest legal rates applicable;

(vi) appropriate injunctive relief;

(vii) attorneys' fees and litigation expenses;

(viii) costs of suit; and

(ix) such other and further relief that the Court deems just and proper.

DEMAND FOR JURY TRIAL

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

Respectfully submitted,

Dated: June 11, 2019

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
THOMAS J. O'REARDON II (247952)
JENNIFER L. MACPHERSON (202021)

By: *s/ Timothy G. Blood*
TIMOTHY G. BLOOD
501 West Broadway, Suite 1490

San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
toreardon@bholaw.com
jmacpherson@bholaw.com

Attorneys for Plaintiff

ClassAction.org