Exhibit C14

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

WENDY WALLACH, individually and on behalf of all others similarly situated, Plaintiff, v. LABORATORY CORPORATION OF AMERICA HOLDINGS Defendant.	Civil Action No. **COMPLAINT and DEMAND FOR JURY TRIAL**

Plaintiff Wendy Wallach ("Plaintiff") individually and on behalf of those similarly situated, brings this class action lawsuit against Laboratory Corporation of America Holdings ("LabCorp" or "Defendant") based upon personal knowledge as to herself, the investigation of her counsel, and on information and belief as to all other matters.

INTRODUCTION

1. Plaintiff, individually and on behalf of all others similarly situated, brings this class action on behalf of all persons whose personal information was compromised as a direct result of Defendant's failure to safeguard millions of patients' highly sensitive medical, personal, and financial information.

2. LabCorp is one of the largest medical testing providers in the country. According to LabCorp's 2018 Annual Report, LabCorp processes approximately "2.5 million patient specimens each week and has laboratory locations throughout the U.S."[1] In providing its

[1] *See* Laboratory Corporation of America Holdings, Annual Report (Form 10-K) (02/28/2019).

services, LabCorp collects its customers' medical, personal, and financial information. Plaintiff, like millions of other consumers, entrusted their sensitive medical, personal, and financial information to LabCorp when they retained LabCorp for diagnostic services.

3. LabCorp uses American Medical Collection Agency, Inc. ("AMCA") as one of its billing collection agencies. LabCorp "has referred approximately 7.7 million consumers to AMCA whose data was stored in the affected AMCA system."[2] AMCA stores consumers' "first and last name, date of birth, address, phone, date of service, provider, and balance information."[3] AMCA's "system also included credit card or bank account information."[4]

4. On June 4, 2019, LabCorp revealed, through its Form 8-K filing with the Securities and Exchange Commission ("SEC"), that an unauthorized user had access to AMCA's system that contained personally identifiably information ("PII") and protected health information ("PHI") (collectively, "PII and PHI") of nearly 7.7 million of LabCorp's patients. The PII and PHI accessed included, but was not limited to, Plaintiff's and Class members' personal information (including addresses, phone numbers, names, and date of birth), financial information (including credit card numbers and bank account information), and personal medical information. LabCorp further revealed that the exposure occurred between August 1, 2018 and March 30, 2019.

5. At all relevant times, LabCorp promised and agreed—throughout its Notice of Privacy Practices and other written assurances—to safeguard and protect PII and PHI in accordance with Health Insurance Portability and Accountability Act ("HIPAA") regulations, federal, state and local laws, and industry standards. Specifically, LabCorp tells its patients that

[2] *See* Laboratory Corporation of America Holdings, Current Report (Form 8-K) (06/04/2019).
[3] *Id.*
[4] *Id.*

it is "committed to protection of your PHI [Protected Health Information] and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation."[5] Moreover, LabCorp promises that any "business associates" to which LabCorp may provide its customers' PII and PHI, are required to maintain the privacy and security of the data.[6]

6. Contrary to those promises, and despite the fact that the threat of a data breach has been a well-known risk to Defendant, especially due to the valuable and sensitive nature of the data maintained by Defendant, Defendant failed to take the reasonable steps to adequately protect the PII and PHI of millions of its patients. The data breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect PII and PHI.

7. Plaintiff and the Class members would not have provided their PII and PHI to Defendant if Plaintiff and Class members knew that Defendant would breach its promises by failing to ensure that its vendors used adequate security measures.

8. As a result of Defendant's failure to take reasonable steps to adequately protect the ultra-sensitive PII and PHI of its millions of patients, Plaintiff's and Class members' PII and PHI is now in the hands of thieves.

9. Defendant's failure to implement and follow basic security procedures 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 fraud that could result in significant monetary loss.

---

[5] *See Notice of Privacy Practices*, LabCorp, (Revised April 18, 2016) *available at* https://www.labcorp.com/hipaa-privacy/hipaa-notice-privacy-practices# (last accessed 7/1/2019).
[6] *Id.*

10. Accordingly, Plaintiff seeks to recover damages and other relief resulting from the data breach, including but not limited to, compensatory damages, reimbursement of costs that she and others similarly situated will be forced to bear, and declaratory and injunctive relief to mitigate future harms that are certain to occur in light of the scope of this breach.

JURISDICTION AND VENUE

11. The Court has jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because at least one member of the Class is a citizen of a state different from the Defendant, the amount in controversy exceeds $5,000,000 exclusive of interest and costs, the Class contains more than 100 members, and none of the exceptions under the subsection applies to this action.

12. The Court has supplemental jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367(a),

13. This Court has personal jurisdiction over Defendant because it is registered to and regularly conducts 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.

14. 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 Plaintiff resides in this District.

THE PARTIES

15. Plaintiff Wendy Wallach is an individual residing in Orange County, New York, and a patient of LabCorp. Her personal information, including PII and PHI, was compromised in the data breach described herein as set forth in a notification letter she received on or around

June 13, 2019 from Retrieval-Masters Creditors Bureau, Inc. d/b/a AMCA. As a result of the data breach, Plaintiff Wallach has been actively monitoring her financial and personal accounts in an effort to detect and prevent any misuses. Plaintiff Wallach would not have gone to LabCorp and used LabCorp's services had Defendant disclosed that it lacked adequate computer systems and data security practices, including the monitoring of vendors, to safeguard her PII and PHI from theft.

16. Defendant Laboratory Corporation of America Holdings is a Delaware corporation with its principal place of business in Burlington, North Carolina.

FACTUAL ALLEGATIONS

A. LabCorp's Services

17. LabCorp touts itself as "The World's Leading Health Care Diagnostics Company."[7] LabCorp "provides diagnostic, drug development and technology-enabled solutions for more than 120 million patient encounters per year,"[8] and "processes tests on more than 2.5 million patient specimens per week."[9] LabCorp provides medical diagnostic testing services in order to "improve health and improve lives by delivering world-class diagnostics."[10] LabCorp's testing services include: blood tests, urine tests, health screening and monitoring tests, drug screening and testing.[11]

[7] *See LabCorp Home Page*, https://www.labcorp.com (last accessed July 2, 2019).
[8] *See LabCorp About Us Page*, https://www.labcorp.com/about-us (last accessed July 2, 2019).
[9] *Id.*
[10] *Id.*
[11] *See LabCorp Services Page*, https://www.labcorp.com/labs-and-appointments/labcorp-services (last accessed July 2, 2019).

18. LabCorp asks its customers to bring to their appointment photo identification, current health insurance information, and a method of payment.[12]

19. LabCorp charges for the laboratory services it provides to its patients. The invoices LabCorp sends are laboratory testing fees which "patients may be responsible for some or all of the costs associated with laboratory testing."[13] If a patient's insurance does not cover the services or if a patient is uninsured, then the patient is responsible for payment of the invoice.

20. If a customer does not pay their invoice within the requested period, their bill will be sent to a collection agency. LabCorp uses AMCA as one of its billing collection agencies in order to facilitate the bill collection process.

21. Upon information and belief, LabCorp provided AMCA with LabCorp's patients' PII and PHI.

B. Defendant Promised to Protect its Customers' Personal Information

22. LabCorp maintains a Notice of Privacy Practices on its website ("Privacy Practices") and states that it is required by law to maintain the privacy of its customers' protected health information. Specifically, LabCorp states that:

> Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), LabCorp is required by law to maintain the privacy of health information that identifies you, called protected health information (PHI), and to provide you with notice of our legal duties and privacy practices regarding PHI. LabCorp is committed to the protection of your PHI and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation. We take this commitment seriously and will work with you to comply with your right to receive certain information under HIPAA.[14]

---

[12] *See LabCorp What to Expect Page*, https://www.labcorp.com/labs-and-appointments/what-to-expect (last accessed July 2, 2019).
[13] *See LabCorp Patient Bill Pay Page*, https://www.labcorp.com/bill-pay (last accessed July 2, 2019).
[14] *See Notice of Privacy Practices*, LabCorp, *available at* https://www.labcorp.com/hipaa-privacy/hipaa-information (last accessed July 1, 2019).

23. LabCorp also ensures its customers that it will only use its customers' personal information for certain limited purposes, such as for treatment, payment, or healthcare operations purposes and for other purposes permitted or required by law.[15]

24. Moreover, LabCorp further provides the following:

> For purposes not described above, including uses and disclosures of PHI for marketing purposes and disclosures that would constitute a sale of PHI, LabCorp will ask for patient authorization before using or disclosing PHI. If you signed an authorization form, you may revoke it, in writing, at any time, except to the extent that action has been taken in reliance on the authorization.[16]

25. Accordingly, Defendant was aware of its obligations and duties to protect its patients' PII and PHI, as evidenced by the statements made on its website.

C. The Data Breach

26. On June 4, 2019, in a filing with the Securities and Exchange Committee ("SEC"), LabCorp disclosed that AMAC had notified LabCorp of the existence of a massive data breach affecting AMCA's web payment page comprising the personal information of 7.7 million LabCorp patients. Specifically, in the Form 8-K, LabCorp stated that:

- between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA's web payment page that contained information that AMCA had received from various entities, including LabCorp;

- the information on AMCA's affected system included first and last name, date of birth, address, phone, date of service, provider, balance information, credit card and bank account information.[17]

[15] *Id.*
[16] *Id.*
[17] *See* Laboratory Corporation of America Holdings, Current Report (Form 8-K) (06/04/2019).

27. LabCorp further stated that "AMCA has informed LabCorp that it is in the process of sending notices to approximately 200,000 LabCorp consumers whose credit card or bank account information may have been accessed. AMCA has not yet provided LabCorp a list of the affected LabCorp consumers or more specific information about them."[18]

28. Accordingly, for approximately eight months, unauthorized parties maintained uninterrupted access to the AMCA system, containing financial information (e.g., credit card numbers and bank account information), medical information and other personal information, of nearly 7.7 million of LabCorp's customers.

29. LabCorp should have known about the data breach no later than March 2019. However, instead of making a public announcement so its customers would know, LabCorp simply disclosed the data breach through an SEC filing.

30. LabCorp collects and stores an enormous amount of PII and PHI that it provides to its vendors such as AMCA to further its business. Despite understanding the consequences of inadequate data security, Defendant failed to take appropriate protective measures to protect and secure the PII and PHI of nearly 7.7 million people, and to ensure that its vendors take appropriate measures to protect and secure the PII and PHI of nearly 7.7 million people.

D. <u>The Data Breach was a Foreseeable Risk of which Defendant was on Notice</u>

31. Identity thieves and cyber criminals have targeted the medical industry in the last several years given the treasure trove of ultra-sensitive personal data stored on these systems.

32. The medical industry is rife with examples of hackers targeting users' PII and PHI, including Anthem, Premera, and St. Joseph Health System, among others, all of which predate the time frame Defendant has identified regarding LabCorp data breach at issue.

[18] *Id.*

33. As early as 2014, the FBI alerted healthcare stakeholders that they were the target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[19]

34. In fact, in a Form 10-K filed with the SEC on February 28, 2019, LabCorp acknowledged that it was aware that its systems were subject to cyber attacks.[20] Specifically, LabCorp stated that cyber-attacks could result in "[a] compromise in the Company's security systems, or those of the Company's third party service providers and vendors, that results in customer personal information being obtained by unauthorized persons or the Company's or third party's failure to comply with security requirements for financial transactions could adversely affect the Company's reputation with its customers and others, as well as the Company's results of operations, financial condition and liquidity. It could also result in litigation against the Company and the imposition of fines and penalties."[21]

35. Accordingly, LabCorp knew, given the vast amount of PII and PHI they managed and maintained, that they were a target of security threats, and therefore understood the risks posed by their insecure data security practices and systems. Defendant's failure to heed warnings and to otherwise maintain adequate security practices resulted in this data breach.

---

[19] *See FBI warns healthcare firms they are targeted by hackers,* Reuters (Aug. 20, 2014), *available at* http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U201 40820 (last accessed June 11, 2019).
[20] *See* Laboratory Corporation of America Holdings, Annual Report (Form 10-K) (02/28/2019).
[21] *Id.*

E. Defendant, At All Relevant Times, Had A Duty To Plaintiff And Class Members To Properly Secure Their PII and PHI

36. Defendant, at all relevant times, had a duty to Plaintiff and Class members to properly secure their PII and PHI, encrypt and maintain such information using industry standard methods, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harms to Plaintiff and Class members, and promptly notify customers when Defendant became aware of the potential that its customers' PII and PHI may have been compromised.

37. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and the other Class members, on the other hand. The special relationship arose because Plaintiff and the members of the Classes entrusted Defendant with their PII and PHI as part of receiving or paying for laboratory services, which are confidential in nature. Defendant had the resources necessary to prevent the data breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached common law, statutory and other owed duties to Plaintiff and Class members.

38. Defendant's duty to use reasonable security measures also arose under HIPAA. Under HIPAA, Defendant was 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.

39. Defendant's duty to use reasonable security measures also arose 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 Defendant.

40. The data breach was a direct and proximate result of Defendant's failure to: (1) properly safeguard and protect Plaintiff's and Class members' PII and PHI from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (2) establish and implement appropriate safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII and PHI; and (3) protect against reasonably foreseeable threats to the security or integrity of such information.

F. Plaintiff and Class Members Were Grievously Harmed By The Data Breach

41. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[22] According to the FTC, identity thieves use stolen personal information for a variety of crimes, including draining bank accounts, credit card fraud, phone or utilities fraud, and even tax fraud."[23]

42. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves can use stolen personal information to open financial accounts and incur charges and credit in a person's name.[24] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

[22] 17 C.F.R. § 248.201 (2013).
[23] *See Warning Signs of Identity Theft,* Federal Trade Commission (May 2015), *available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited July 2, 2019).
[24] *See* https://www.gao.gov/new.items/d07737.pdf (last visited July 2, 2019).

43. Accordingly, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[25]

44. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web 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.[26]

45. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[27]

46. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

47. For all of the above reasons, Plaintiff and the Class members have suffered harm; and there is a substantial risk of injury to Plaintiff and the Class members that is imminent and concrete and that will continue for years to come.

---

[25] *Guide for Assisting Identity Theft Victims*, Federal Trade Commission (September 2013), *available at* http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited June 11, 2019)

[26] GAO Report at 29.

[27] *See Study: Medical identity theft is costly for victims,* CNET (Mar. 3, 2010), *available at* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed June 11, 2019).

48. As a direct and proximate result of Defendant's wrongful actions and inaction, Plaintiff and Class members have suffered injury and damages, including the increased risk of identity theft and identity fraud, improper disclosure of PII and PHI, the time and expense necessary to mitigate, remediate, and sort out the increased risk of identity theft and the inability to use debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the data breach, and/or false or fraudulent charges stemming from the data breaches.

CLASS ACTION ALLEGATIONS

49. Plaintiff brings this action on behalf of himself and on behalf of two classes – a Nationwide Class and a New York Subclass (together "Classes" or "Class Members") pursuant to the Federal Rule of Civil Procedure 23(b)(2) and (b)(3).

50. The Nationwide Class is defined as follows: All persons in the United States whose PII and PHI were maintained on the AMCA systems that were compromised as a result of the breach announced by LabCorp on or around June 4, 2019.

51. The New York Subclass is defined as follows: All persons in the State of New York whose PII and PHI were maintained on the AMCA systems that were compromised as a result of the breach announced by LabCorp on or around June 4, 2019.

52. Excluded from the proposed Classes are: Defendant, any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant; and judicial officers to whom this case is assigned and their immediate family members.

53. Plaintiff reserves the right to re-define the Class definitions after conducting discovery.

54. **Numerosity (Fed. R. Civ. P. 23(a)(1)**. The Class Members are so numerous that joinder of all members is impracticable. Based on information and belief, the Classes include nearly 7.7 million individuals from across the country who had their PII and PHI compromised during the data breach. The parties will be able to identify the exact size of the Classes through discovery and Defendant's own documents.

55. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2); 23(b)(3))**. Common questions of law and fact exist with regard to each of the claims and predominate over questions affecting only individual members of the Classes. Questions common to the Classes include, but not limited to the following:

a. Whether Defendant had a legal duty to implement and maintain reasonable security procedures and practices for the protection of Class members' PII and PHI, including by vendors;

b. Whether Defendant breached its legal duty to implement and maintain reasonable security procedures and practices for the protection of Class members' PII and PHI;

c. Whether Defendant's conduct, practices, actions, and omissions, resulted in or was the proximate cause of the data breach, resulting in the loss of PII and PHI of Plaintiff and Class members;

d. Whether Defendant had a legal duty to provide timely and accurate notice of the data breach to Plaintiff and Class members;

e. Whether Defendant breached its duty to provide timely and accurate notice of the data breach to Plaintiff and Class members;

f. Whether and when Defendant knew or should have known that AMCA's computer systems were vulnerable to attack;

g. Whether Defendant failed to implement and maintain reasonable and adequate security measures, procedures, and practices to safeguard Class members' PII and PHI, including by vendors;

h. Whether Defendant's practices, actions, and omissions constitute unfair or deceptive business practices;

i. Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendant's conduct, including increased risk of identity theft and loss of value of their PII and PHI; and

j. Whether Plaintiff and Class members are entitled to relief, including damages and equitable relief.

56. **Typicality (Fed. R. Civ. P. 23(a)(3))**. Pursuant to Rule 23(a)(3), Plaintiff's claims are typical of the claims of the Class members. Plaintiff, like all Class members, had her PII and PHI compromised in the data beach.

57. **Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)**. Pursuant to Rule 23(a)(4), Plaintiff and her counsel will fairly and adequately protect the interests of the Classes. Plaintiff has no interest antagonistic to, or in conflict with, the interested of the Class members. Plaintiff has retained counsel experienced in prosecuting class actions and data breach cases.

58. **Superiority (Fed. R. Civ. P. 23(b)(3)**. Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual Class members because the amount of monetary relief available to individual plaintiffs is insufficient in the absence of the class action procedure. Separate litigation could

yield inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

59. **Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)).** In the alternative, this action may properly be maintained as a class action, because:

a. the prosecution of separate actions by individual members of the Classes would create a risk of inconsistent or varying adjudication with respect to individual Class members which would establish incompatible standards of conduct for Defendant; or

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

60. Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Classes as a whole.

61. **Issue Certification (Fed. R. Civ. P. 23(c)(4).** In the alternative, the common questions of fact and law, set forth in Paragraph 55, are appropriate for issue certification on behalf of the proposed Classes.

COUNT I

NEGLIGENCE

(On Behalf of the Nationwide Class)

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

63. LabCorp required Plaintiff and Class members to submit non-public, sensitive PII and PHI to obtain medical services, which LabCorp provided to AMCA for billing purposes.

64. Defendant had (and continues to have) a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII and PHI. Defendant also had (and continues 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 PII and PHI within their possession, custody and control) and that of its vendors.

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

66. Defendant violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII and 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 and PHI entrusted to it – including Plaintiff's and Class members' PII and PHI. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII and 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 and PHI.

67. Defendant, by and through its negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its 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 and PHI within their possession, custody and control.

68. Defendant, by and through its negligent actions, inactions, omissions, and want of ordinary care, further breached its duties to Plaintiff and Class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their PII and PHI.

69. But for Defendant's negligent breach of the above-described duties owed to Plaintiff and Class members, their PII and PHI would not have been released, disclosed, and disseminated without their authorization.

70. Plaintiff's and Class members' PII and 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 Defendant's failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiff's and Class members' PII and PHI.

71. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this data breach constitute negligence.

72. As a direct and proximate result of Defendant's 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) ongoing, imminent, and 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 dark web; 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.

COUNT II

BREACH OF CONTRACT

(On Behalf of the Nationwide Class)

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

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

75. Plaintiff and Class members performed their obligations under the contracts when they provided their PII and PHI to LabCorp for laboratory and diagnostic services and when they paid for the service provided by LabCorp.

76. LabCorp breached its contractual obligations to protect the nonpublic personal information LabCorp possessed and was entrusted with when the information was accessed by unauthorized persons as part of the data breach.

77. As a direct and proximate result of LabCorp's above-described breach of contract, Plaintiff and Class members have suffered (and will continue to suffer) ongoing, imminent, and 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 dark web; 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.

COUNT III

BREACH OF IMPLIED CONTRACT

(On Behalf of the Nationwide Class)

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

79. Defendant provided Plaintiff and Class members with an implied contract to protect and keep private their PII and PHI.

80. Plaintiff and Class members would not have provided their PII and PHI to Defendant or its vendors, but for Defendant's implied promises to safeguard and protect their information.

81. Plaintiff and Class members performed their obligations under the implied contract when they provided their PII and PHI to LabCorp for laboratory and diagnostic services and when they paid for the service provided by LabCorp.

82. Defendant breached the implied contract with Plaintiff and Class members by failing to protect and keep private their PII and PHI.

83. As a direct and proximate result of LabCorp's above-described breach of implied contract, Plaintiff and Class members have suffered (and will continue to suffer) ongoing, imminent, and 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 dark web; 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.

COUNT IV

VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW § 349

(On Behalf of the New York Subclass)

84. Plaintiff realleges and incorporates by reference each of the allegations set forth above.

85. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Defendant misrepresented and fraudulently advertised material facts, pertaining to the sale and/or furnishing of services, to the New York Subclass by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard New York Class Members' PII and PHI from unauthorized disclosure, release, data breaches and theft;

b. Defendant misrepresented material facts, pertaining to the sale and/or furnishing of services, to the New York Subclass by representing and advertising that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of New York Class Members' Personal Information;

c. Defendant omitted, suppressed, and concealed material fact of the inadequacy of its privacy and security protections for New York Class Members' PII and PHI;

d. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of New York Class Members' PII and PHI, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and HIPPA (42 U.S.C. § 1302d et. seq.);

e. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the data breach to New York Class Members in a timely

and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

86. Defendant knew or should have known that the AMCA computer systems and data security practices were inadequate to safeguard New York Subclass members' PII and PHI entrusted to it, and that risk of a data breach or theft was highly likely.

87. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

88. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and New York Subclass members) regarding the security of AMCA's network and aggregation of PII and PHI.

89. The representations upon which consumers (including Plaintiff and New York Subclass members) relied were material representations (*e.g.*, as to Defendant's adequate protection of PII and PHI), and consumers (including Plaintiff and New York Subclass members) relied on those representations to their detriment.

90. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class members have been harmed, in that they were not timely notified of the data breach, which resulted in profound vulnerability to their personal information and other financial accounts.

91. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and New York Subclass members' PII and PHI was

disclosed to third parties without authorization, causing and will continue to cause Plaintiff and New York Subclass members damages.

92. Plaintiff and New York Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

DEMAND FOR JURY TRIAL

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

DATED: July 3, 2019

LEVI & KORSINSKY, LLP

/s/ Eduard Korsinsky

Eduard Korsinsky (EK-8989)
Courtney E. Maccarone (CM-5863)
55 Broadway, 10th Floor
New York, NY 10006
Tel: (212) 363-7500
ek@zlk.com
cmaccarone@zlk.com

LEVI & KORSINSKY LLP
Rosemary M. Rivas*
rrivas@zlk.com
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Tel: (415) 373-1671
rrivas@zlk.com

**Pro Hac Vice Application Forthcoming*

Attorneys for Plaintiff and Proposed Classes