# Exhibit C17

**UNITED STATES DISTRICT COURT**
**FOR THE SOUTHERN DISTRICT OF NEW YORK**

CLYDE FREEMAN and TIM COLLINSWORTH, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

AMERICAN MEDICAL COLLECTION AGENCY, INC.; LABORATORY CORPORATION OF AMERICA HOLDINGS; CLINICAL PATHOLOGY LABORATORIES, INC.; BIO-REFERENCE LABORATORIES, INC.; and DOES 1-10,

Defendants.

Case No. 7:19-cv-06853

**CLASS ACTION COMPLAINT**

Jury Trial Demanded

Plaintiffs Clyde Freeman and Tim Collinsworth, on behalf of themselves and all others similarly situated, through the undersigned counsel, hereby allege the following, against Defendants American Medical Collection Agency, Inc., ("AMCA"), Laboratory Corporation of America Holdings ("LabCorp"), Clinical Pathology Laboratories, Inc. ("CPL"), and Bio-Reference Laboratories, Inc. (Bio-Reference) (collectively, "Defendants"), upon their own knowledge or, where they lack personal knowledge, upon information and belief including the investigation of their counsel, as follows:

## I. INTRODUCTION

1. Plaintiffs bring this class action on behalf the proposed Classes defined below, against Defendants because of their failure to protect the confidential information of millions of patients—including financial information (e.g., credit card numbers and bank account information), medical information, personal information (e.g., Social Security Numbers), and/or other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, their "Sensitive Information"). Defendants' wrongful disclosure has harmed Plaintiffs.

## II. PARTIES

2. Plaintiff Clyde Freeman is an individual residing in Walden, New York, who has been a patient of Laboratory Corporation of America, and Bio-Reference Laboratories, Inc., and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

3. Plaintiff Tim Collinsworth is an individual residing in Catoosa, Oklahoma, who has been a patient of Clinical Pathology Laboratories, Inc. and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

4. Defendant American Medical Collection Agency, Inc. is a New York Corporation with its principal place of business in Elmsford, New York.

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

6. Defendant Clinical Pathology Laboratories, Inc. is a Texas Corporation with its principal place of business in Austin, Texas.

7. Defendant Bio-Reference Laboratories, Inc. is a New Jersey corporation with its principal place of business in Elmwood Park, New Jersey.

## III. JURISDICTION AND VENUE

8. Subject Matter Jurisdiction. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) in that: (1) this is a class action involving more than 1,000 class members; (2) minimal diversity is present as Plaintiff Freeman is a citizen of New York, and Plaintiff Collinsworth is a citizen of Oklahoma (and the proposed class members are from various states), while Defendants are citizens of the States of New Jersey, North Carolina, Texas, and New York; and (3) the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs.

9. Personal Jurisdiction. This Court has personal jurisdiction over Defendants because Defendants do business in and throughout the State of New York, and the wrongful acts alleged in this Complaint were committed in New York, among other venues.

10. Venue. Venue is proper in this District pursuant to: (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, and 28 U.S.C. § 1391(d) because the transactions giving rise to the claims occurred in

Orange County, New York; and (2) 28 U.S.C. § 1391(b)(3) in that Defendants are subject to personal jurisdiction in this District.

## IV. FACTUAL ALLEGATIONS

### Laboratory Corporation of America Holdings

11. Laboratory Corporation of America Holdings ("LabCorp") is a leading provider of diagnostic, drug development and capabilities, and provides comprehensive laboratory and end-to-end drug development services worldwide.[1]

12. LabCorp performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease. LabCorp boasts of over 2,000 locations and more than 6,000 in-office phlebotomists located in customer offices and facilities, and "typically processes tests on more than 2.5 million patient specimens each week."[2]

13. LabCorp maintains a Notice of Privacy Practices on its website[3], which provides among other things, that "[u]nder the Health Insurance Portability and Accountability Act of 1996 (HIPAA), LabCorp is required by law to maintain the privacy of health information that identifies [its patients] . . . and to provide [them] with notice of [LabCorp's] legal duties and privacy practices regarding PHI." Further, LabCorp states that it "is committed to the protection of [its patients'] PHI and will make reasonable efforts to ensure" its confidentiality, "as required by statute and regulation." *Id.* LabCorp also assures its patients that it takes its "commitment seriously."

14. On June 4, 2019, LabCorp publicly announced that its billing collections vendor, AMCA, had been breached—exposing the confidential information of as many as 7.7 million

[1] LabCorp, 10-K SEC filing, *available at* <https://www.sec.gov/Archives/edgar/data/920148/000092014819000033/lh10-k2018.htm> (last visited July 22, 2019).
[2] *Id.*
[3] https://www.labcorp.com/hipaa-privacy/hipaa-information (last visited July 22, 2019).

LabCorp patients whose data was stored in the affected system.[4] According to LabCorp, the information consisted of its customers' "first and last name, date of birth, address, phone, date of service, provider, and balance information. [The] [] affected system also included credit card or bank account information that was provided by the consumer to AMCA (for those who sought to pay their balance)" (the "Data Breach"). According to LabCorp, the Data Breach occurred between August 1, 2018 and March 30, 2019.

15. LabCorp further admitted 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.[5]

16. But, at the end of February 2019, Gemini Advisory analysts had disclosed a data breach at AMCA that affected approximately 200,000 customers:

> On 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.[6]

17. This exposure "lasted for at least seven months beginning September, 2018, and had affected more than 200,000 victims."[7] However, when Gemini Advisory attempted to notify AMCA on March 1, 2019, it received no response.[8]

---

[4] LabCorp, Form 8-K, dated June 4, 2019 *available at* <https://www.sec.gov/Archives/edgar/data/920148/000119312519165091/d757830d8k.htm> (last visited July 22, 2019).

[5] *Id.*

[6] Databreaches.net, "American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory," *available at* <https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/> (last visited July 22, 2019).

[7] *Id.*

[8] *Id.*

18. AMCA states that, on March 20, 2019,[9] it received "information from a security compliance firm that works with credit card companies of a possible security compromise" and, after conducting "an internal review . . . took down" its web payments page.[10] AMCA did not provide identifying information for the security compliance firm that notified it of the "security compromise."

19. LabCorp's June 4, 2019 filing does not indicate that there were any communications between AMCA and LabCorp concerning the Gemini Advisory notification or any other communications concerning the Data Breach at any point prior to June 4, 2019.

**Clinical Pathology Laboratories, Inc.**

20. Clinical Pathology Laboratories, Inc. ("CPL") touts itself as offering the highest quality laboratory services dedicated to the individual needs of practitioners and their patients.

21. On July 12, 2019, CPL announced via its website[11] that it had been informed by Retrieval Masters Creditors Bureau d/b/a American Medical Collection Agency ("AMCA") of a data security incident involving the AMCA payment website.[12]

22. According to CPL, "on March 21, 2019, AMCA became aware of facts indicating there had been a data security incident," and that, after AMCA's investigation in May of 2019, "AMCA notified CPL about the incident and informed CPL that an AMCA database containing information for some CPL patients had been affected." *Id.*

23. CPL disclosed that "at the time of AMCA's initial notification, AMCA did not provide CPL with enough information for CPL to identify potentially affected patients or

---

[9] "#12625934: BioReference Laboratories Added to AMCA Breach Tally," *available at* < https://brica.de/alerts/alert/public/1262594/bioreference-laboratories-added-to-amca-breach-tally/> (last visited July 22, 2019).

[10] KrebsonSecurity, "LabCorp: 7.7 Million Consumers Hit in Collections Firm Breach (June 4, 2019), *available at* <https://krebsonsecurity.com/2019/06/labcorp-7-7m-consumers-hit-in-collections-firm-breach/> (last visited July 22, 2019).

[11] https://www.cpllabs.com/about-us/announcements/ (last visited July 22, 2019).

[12] "Clinical Pathology Laboratories, Inc. Notifies Patients of Data Security Incident" *available at* <https://www.prnewswire.com/news-releases/clinical-pathology-laboratories-inc-notifies-patients-of-data-security-incident-300885218.html> (last visited July 22, 2019).

confirm the nature of patient information potentially involved in the incident." *Id.* CPL added that its investigation is on-going, and that "[b]ased on the information provided by AMCA, the following information belonging to CPL patients may have been affected by the incident: patient names, addresses, phone numbers, dates of birth, dates of service, balance information, credit card or banking information and treatment provider information." *Id.*

24. Although CPL knew of the Data Breach at least as of May 2019, on information and belief CPL did not take any steps to notify patients whose information was affected until July 2019, approximately two months after CPL was made aware of it.

25. CPL maintains a Patient Privacy Policy on its website wherein it acknowledges, among other things, that it is required to "[m]aintain the privacy and security of [its patients'] health information," and that it is required to "[i]nform [its patients] if a breach occurs that may have compromised the privacy or security of [its patients'] information."[13]

**Bio-Reference Laboratories, Inc.**

26. Bio-Reference Laboratories, Inc. ("Bio-Reference"), a subsidiary of OPKO Health Inc., is a large medical testing provider. Bio-Reference collects private personal, medical, and financial information from its patients. Bio-Reference utilizes AMCA for billing collection services. AMCA obtains and shares Bio-Reference patients' Sensitive Information, and is charged with safeguarding that Sensitive Information.

27. Bio-Reference maintains a Notice of Privacy Practices on its website,[14] which provides:

> BioReference Laboratories, Inc. and its subsidiaries and divisions, including but not limited to, GeneDx, Inc., Florida Clinical Laboratory, Inc., and GenPath (collectively "BRLI) are committed to complying with and addressing data protection requirements under all laws that apply to our business, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA) ….

[13] https://www.cpllabs.com/patients/policies/ (last visited July 22, 2019).
[14] Bio-Reference, "Notice of Privacy Practices". *See* https://www.bioreference.com/wp-content/uploads/2019/02/NOPP-BRLI-January-2019.pdf (last visited July 22, 2019).

28. On June 3, 2019, Bio-Reference revealed in an 8-K filing[15] with the Securities and Exchange Commission that unauthorized parties had access to AMCA's systems. Bio-Reference revealed that it was advised by AMCA that data for approximately 422,600 patients for whom Bio-Reference performed testing was stored in the affected AMCA system. *Id.*

29. AMCA also advised Bio-Reference that the affected AMCA system includes information provided by Bio-Reference that may have included patient name, date of birth, address, phone, date of service, provider, and balance information. *Id.* In addition, the affected AMCA system also included credit card information, bank account information and email addresses that were provided by the consumer to AMCA.

30. Bio-Reference's June 3, 2019 filing does not indicate that there were any communications between AMCA and Bio-Reference concerning the Gemini Advisory notification or any communications regarding the Data Breach at any point prior to June 3.

**American Medical Collection Agency**

31. AMCA claims that it is "compliant with all Federal and State Laws," and, further, provides its "services adhering to the ethical guidelines expected from a National Accounts Receivable Management firm."[16]

32. Although Defendants should have known of the Data Breach not later than March 2019, and although AMCA knew of the breach earlier, none of the Defendants took any steps to notify patients whose information was affected until at least June 3, 2019 and only in SEC filings.

[15] OPKO Health, Inc. From 8-K SEC, *available at* <https://www.sec.gov/Archives/edgar/data/944809/000094480919000039/a8-kbrli6x6x19.htm> (last visited

[16] AMCA, "An Industry Leader," *available at* < http://amcaonline.com/about.php> (last visited July 22, 2019).

**Defendants Had Obligations to Protect Their Patients' Sensitive Information**

33. Defendants had obligations created by HIPAA, arising from promises made to patients like Plaintiffs and other Class members, and based on industry standards, to keep the compromised Sensitive Information confidential and to protect it from unauthorized disclosures. Class members provided their Sensitive Information to Defendants with the understanding that Defendants and any business partners to whom Defendants disclosed the Sensitive Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

34. Defendants' data security obligations and promises were particularly important given the substantial increase in data breaches — particularly those in the healthcare industry — preceding August 2018, which were widely known to the public and to anyone in Defendants' industries.

35. Defendants' security failures demonstrate that they failed to honor their duties and promises by not:

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protecting Plaintiffs' and the Classes' Sensitive Information;

c. Ensuring the confidentiality and integrity of electronic protected health information they created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implementing technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implementing policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implementing procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protecting against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 C.F.R. § 164.306(a)(2);

h. Protecting against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

i. Ensuring compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

j. Training all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

**It is Well Established That Data Breaches Lead to Identity Theft**

36. Plaintiffs and other Class members have been injured by the disclosure of their Sensitive Information in the Data Breach.

37. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in a person's name.[17] As the GAO Report states, this type of identity theft is the most

[17] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* <https://www.gao.gov/new.items/d07737.pdf> (last visited July 22, 2019).

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.

38. 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."[18]

39. Identity theft victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such as social security numbers ("SSNs") for a variety of crimes, including credit card fraud, phone or utilities fraud, and/or bank/finance fraud.

40. There may be a time lag between when Sensitive Information is stolen and when it is used. 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.[19]

41. With access to an individual's Sensitive Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name. Identity thieves may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[20]

---

[18] *Id.* at 2, 9.
[19] *Id*. at 29 (emphasis added).
[20] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited July 22, 2019).

42. Sensitive Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other Sensitive Information directly on various Internet websites making the information publicly available.

43. 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.[21] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

44. Medical databases are especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value — whereas a stolen social security number, on the other hand, only sells for $1."[22] In fact, the medical industry has experienced disproportionally higher instances of identity theft than any other industry.

## V. CLASS ACTION ALLEGATIONS

45. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs bring this case as a class action on behalf of a Nationwide Class, or in the alternative, on behalf of a New York Sub-Class, defined as follows:

[21] *See* Elinor Mills, Study: Medical identity theft is costly for victims, CNET (Mar. 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last visited Jul 22, 2019).
[22] Study: Few Aware of Medical Identity Theft Risk, Claims Journal, http://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited July 22, 2019).

> Nationwide Class: All persons in the United States whose Sensitive Information was provided to AMCA by LabCorp, CPL, Bio-Reference, and/or other laboratories and maintained on the AMCA systems that were compromised as a result of the breach announced on or around June 4, 2019.
>
> Alternative New York Sub-Class: All persons in the State of New York whose Sensitive Information was provided to AMCA by LabCorp, CPL, Bio-Reference, and/or other laboratories and maintained on the AMCA systems that were compromised as a result of the breach announced on or around June 4, 2019.

Excluded from the above Classes 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.

46. Numerosity. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

47. Commonality. There are numerous questions of law and fact common to Plaintiffs and Class Members. These common questions of law and fact include, but are not limited to, the following:

a. Whether Defendants' data security systems prior to the Data Breach met the requirements of laws including, for instance, HIPAA;

b. Whether Defendants' data security systems prior to the Data Breach met industry standards;

c. Whether Plaintiffs' and other Class members' Sensitive Information was compromised in the Data Breach; and

d. Whether Plaintiffs' and other Class members are entitled to damages as a result of Defendants' conduct.

48. Typicality. Plaintiffs' claims are typical of the claims of the Classes' claims. Plaintiffs suffered the same injury as Class members—*i.e.*, upon information and belief Plaintiffs' Sensitive Information was compromised in the Data Breach.

49. Adequacy. Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs have retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiffs nor their counsel have interests that are contrary to or that conflict with those of the proposed Classes.

50. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and other Class members. The common issues arising from this conduct that affect Plaintiffs and Class members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

51. Superiority. A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class members' interests in individually controlling the prosecution of separate actions is low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendants. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management

difficulties. Defendants' records and the records available publicly will easily identify the Class members. The same common documents and testimony will be used to prove Plaintiffs' claims as well as the claims of other Class members. Finally, proceeding as a class action provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

52. Injunctive and Declaratory Relief Appropriate. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants have acted or refused to act on grounds that apply generally to Class members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class members.

**FIRST CLAIM FOR RELIEF**

**Negligence**

**(On behalf of Plaintiffs and the Nationwide Class)**

53. Plaintiffs reallege and incorporate by reference all preceding factual allegations.

54. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class or, in the alternative, the New York Sub-Class.

55. Defendants required Plaintiffs and Class members to submit non-public Sensitive Information to obtain medical services, which Defendants provided to AMCA for billing purposes.

56. By collecting and storing this data, and sharing it and using it for commercial gain, Defendants accepted a duty of care to use reasonable means to secure and safeguard this Sensitive Information, to prevent disclosure of the information, and to guard the information from theft.

57. Defendants' duty included a responsibility to implement a process by which they could detect a breach of their security systems in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

58. Defendants also owed a duty of care to Plaintiffs and members of the Classes to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that their systems and networks—and the personnel responsible for them—adequately protected their customers' Sensitive Information.

59. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their patients, which is recognized by laws including but not limited to HIPAA. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiffs and the members of the Classes from a data breach.

60. Defendants' duty to use reasonable security measures also arose under HIPAA, pursuant to which Defendants are required to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

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

63. Defendants breached their common law, statutory and other duties—and thus, were negligent—by failing to use reasonable measures to protect patients' Sensitive Information, and by failing to provide timely notice of the Data Breach.

64. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class members' Sensitive Information;

b. failing to adequately monitor the security of AMCA's networks and systems;

c. allowing unauthorized access to Plaintiffs' and Class members' Sensitive Information;

d. failing to recognize in a timely manner that Plaintiffs' and other Class members' Sensitive Information had been compromised; and

e. failing to warn Plaintiffs and other Class members about the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

65. It was foreseeable that Defendants' failure to use reasonable measures to protect Sensitive Information and to provide timely notice of the Data Breach would result in injury to Plaintiffs and other Class members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and the members of the Classes were reasonably foreseeable.

66. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiffs and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time

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

67. Accordingly, Plaintiffs, on behalf of themselves and members of the Classes seek an order declaring that Defendants' conduct constitutes negligence, and awarding damages in an amount to be determined at trial.

**SECOND CLAIM FOR RELIEF**

**Violation of New York General Business Law § 349**

**(On behalf of Plaintiffs and the Nationwide Class)**

68. Plaintiffs reallege and incorporate by reference all preceding factual allegations.

69. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class or, in the alternative, the New York Sub-Class.

70. Defendants, while operating in New York, engaged in deceptive acts and practices in the conduct of business, trade and commerce, and the furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a). This includes but is not limited to the following:

a. Defendants failed to enact adequate privacy and security measures to protect the Class members' Sensitive Information from unauthorized disclosure, release, data breaches, and theft, and this failure was one direct and proximate cause of the Data Breach;

b. Defendants failed to take proper action following known security risks and prior cybersecurity incidents, and this failure was one direct and proximate cause of the Data Breach;

c. Defendants knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard the Sensitive Information from unauthorized disclosure, release, data breaches, and theft;

d. Defendants omitted, suppressed, and concealed the material fact of Defendants' reliance on, and inadequacy of, AMCA's security protections;

e. Defendants knowingly and fraudulently misrepresented that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Sensitive Information, including but not limited to duties imposed by HIPAA; and

f. Defendants failed to disclose the Data Breach to the victims in a timely and accurate manner, in violation of the duties imposed by, *inter alia*, N.Y. Gen Bus. Law § 899-aa(2).

71. As a direct and proximate result of Defendants' practices, Plaintiffs and other Class members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial and medical accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Sensitive Information.

72. The above unfair and deceptive acts and practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and other Class members that they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

73. Defendants knew or should have known that AMCA's computer systems and data security practices were inadequate to safeguard Sensitive Information entrusted to it, and that risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

74. Plaintiffs seek relief under N.Y. Gen. Bus. Law § 349(h), including but not limited to actual damages (to be proven at trial), treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs. The amount of such damages is to be determined at trial, but will not be less than $50.00 per violation.

75. Plaintiffs and Class members seek to enjoin such unlawful deceptive acts and practices described above. Each Class member will be irreparably harmed unless the Court enjoins Defendants' unlawful, deceptive actions in that Defendants will continue to fail to protect Sensitive Information entrusted to them, as detailed herein.

76. Plaintiffs and Class members seek declaratory relief, restitution for monies wrongfully obtained, disgorgement of ill-gotten revenues and/or profits, injunctive relief prohibiting Defendants from continuing to disseminate its false and misleading statements, and other relief allowable under N.Y. Gen. Bus. Law § 349.

**THIRD CLAIM FOR RELIEF**

**Breach of Implied Contract**

**(On Behalf of Plaintiffs and the Nationwide Class)**

77. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

78. Plaintiffs bring this cause of action individually and on behalf of the Nationwide Class or, in the alternative, the New York Sub-Class.

79. When Plaintiffs and Class members paid money and provided their Sensitive Information to Defendants in exchange for services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

80. Defendants solicited and invited prospective clients and other consumers to provide their Sensitive Information as part of its regular business practices. These individuals accepted Defendants' offers and provided their Sensitive Information to Defendants. In entering into such implied contracts, Plaintiffs and the Class assumed that Defendants' data security practices and policies were reasonable and consistent with industry standards, and that Defendants would use part of the funds received from Plaintiffs and the Class to pay for adequate and reasonable data security practices.

81. Plaintiffs and the Class would not have provided and entrusted their Sensitive Information to Defendants in the absence of the implied contract between them and Defendants to keep the information secure.

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

83. Defendants breached their implied contracts with Plaintiffs and the Class by failing to safeguard and protect their Sensitive Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

84. As a direct and proximate result of Defendants' breaches of their implied contracts, Plaintiffs and the Class sustained actual losses and damages as described herein.

## VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on their own behalf and on behalf of Class members, pray for judgment against Defendant as follows:

A. Certification of the proposed Classes;

B. Appointment of Plaintiffs as Class representatives;

C. Appointment of the undersigned counsel as counsel for the Classes;

D. Declaring that Defendants' actions, as described above, constitute negligence and amounted to violations of HIPAA, and the consumer protection laws of New York;

H. An award to Plaintiffs and the Classes of damages, as allowed by law;

I. An award to Plaintiffs and the Classes of attorneys' fees and costs, as allowed by law and/or equity;

J. Leave to amend this Complaint to conform to the evidence presented at trial; and

K. Orders granting such other and further relief as the Court deems necessary, just, and proper.

## VII. DEMAND FOR JURY

Plaintiffs demand a trial by jury for all issues so triable.

Respectfully submitted,

Dated: July 23, 2019

/s/ Tina Wolfson
Tina Wolfson
*twolfson@ahdootwolfson.com*
Bradley K. King
*bking@ahdootwolfson.com*
Theodore W. Maya (*pro hac vice* forthcoming)
*tmaya@ahdootwolfson.com*
**AHDOOT & WOLFSON, PC**
125 Maiden Lane, Suite 5C
New York, New York 10038
Tel: 917-336-0171
Fax: 917-336-0177

Russell Yankwitt
*russell@yankwitt.com*
Michael H. Reed
*michael@yankwitt.com*
**YANKWITT LLP**
140 Grand Street, Suite 705
White Plains, New York 10601
Tel: 914-686-1500
Fax: 914-487-5000

*Counsel for Plaintiffs and the Putative Classes*