Exhibit C19

James E. Cecchi
Lindsey H. Taylor
Caroline F. Bartlett
CARELLA BYRNE CECCHI
OLSTEIN BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
(973) 994-1700

Attorneys for Plaintiffs
(Additional Counsel on the Signature Page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

VICKI JOHNS, BRIAN LEVY, NAOMI SHAPIRO, and HANNAH WEISS, individually and on behalf of all those similarly situated, Plaintiffs, v. BIO-REFERENCE LABORATORIES, INC., CLINICAL PATHOLOGY LABORATORIES, INC., LABORATORY CORPORATION OF AMERICA HOLDINGS, OPTUM360 SERVICES, INC., and QUEST DIAGNOSTICS, INCORPORATED, Defendants.	Civil Action No. **COMPLAINT and** **DEMAND FOR JURY TRIAL**

Plaintiffs Vicki Johns, Brian Levy, Naomi Shapiro, and Hannah Weiss ("Plaintiffs"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby allege the following, against Defendants Bio-Reference Laboratories, Inc. ("Bio-Reference"), Clinical Pathology Laboratories, Inc. ("CPL"), Laboratory Corporation of America Holdings ("LabCorp"), Optum360 Services, Inc. ("Optum360"), and Quest Diagnostics,

Incorporated (collectively, "Defendants"). Based upon personal knowledge, information, belief, and investigation of counsel, Plaintiffs specifically allege as follows:

SUMMARY OF THE CASE

1. Plaintiffs bring this class action on behalf of a nationwide class (the "Class") 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 and the Class.

JURISDICTION AND VENUE

2. 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 Plaintiffs are citizens of Florida, New York and Texas (and the proposed class members are from various states), while Defendants are citizens of Minnesota, New Jersey, New York, North Carolina, and Texas; and (3) the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs.

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

4. 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 (2) 28 U.S.C. § 1391(b)(3) in that Defendants are subject to personal jurisdiction in this District.

PARTIES

5. Plaintiff Vicki Johns is an individual residing in Lubbock, Texas, and a citizen of the state of Texas, who has been a patient of CPL, and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

6. Plaintiff Brian Levy is an individual residing in Woodmere, New York, and a citizen of the state of New York, who has been a patient of Bio-Reference and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

7. Plaintiff Naomi Shapiro is an individual residing in Delray Beach, Florida, and a citizen of the state of Florida, who has been a patient of Quest and LabCorp and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

8. Plaintiff Hannah Weiss is an individual residing in Woodmere, New York, and a citizen of the state of New York, who has been a patient of BioReference and whose Sensitive Information, on information and belief, was compromised in the Data Breach described herein.

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

10. Defendant Clinical Pathology Laboratories, Inc. ("CPL") is a Texas corporation with its principal place of business in Austin, Texas.

11. Defendant Laboratory Corporation of America Holdings ("LabCorp") is a Delaware corporation with its principal place of business in Burlington, North Carolina.

12. Defendant Optum360 Services, Inc. ("Optum360") is a Delaware corporation with its principal place of business in Eden Prairie, Minnesota.

13. Quest Diagnostics Incorporated ("Quest") is a Delaware corporation with its principal place of business in Secaucus, New Jersey.

FACTUAL BACKGROUND

Quest

14. Quest is the world's leading provider of medical diagnostic testing services. It performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease.

15. On June 3, 2019, Quest publicly admitted in a filing with the Securities and Exchange Commission ("SEC") that: "On May 14, 2019, American Medical Collection Agency (AMCA), a billing collections vendor, notified Quest . . . and Optum360 LLC, [Quest's] revenue cycle management provider," of a massive data breach compromising the Sensitive Information of 11.9 million Quest patients, and most likely others (the "Data Breach"). Quest Form 8-K, June 3, 2019.

16. Quest's SEC filing disclosed that, "between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA's system that contained information that AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself[,] . . . include[ing] financial information (e.g., credit card numbers and bank account information), medical information[,] and other personal information (e.g., Social Security Numbers)." *Id.*

LabCorp

17. LabCorp is one of the world's leading providers of medical diagnostic testing services. It performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease. Earlier this year, LabCorp disclosed that

LabCorp Diagnostics processes "2.5 million patient specimens each week and has laboratory locations throughout the U.S." LabCorp Form 10-K, Feb. 28, 2019

18. On June 4, 2019, LabCorp publicly announced the following in a filing with the Securities and Exchange Commission ("SEC"):

> [LabCorp] has been notified by Retrieval-Masters Creditors Bureau, Inc. d/b/a American Medical Collection Agency (AMCA) about unauthorized activity on AMCA's web payment page (the AMCA Incident). According to AMCA, this activity occurred between August 1, 2018, and March 30, 2019. AMCA is an external collection agency used by LabCorp and other healthcare companies. LabCorp has referred approximately 7.7 million consumers to AMCA whose data was stored in the affected AMCA system. AMCA's affected system included information provided by LabCorp. That information could include first and last name, date of birth, address, phone, date of service, provider, and balance information. AMCA's 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).

LabCorp Form 8-K, June 4, 2019.

19. LabCorp further disclosed 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." *Id.*

20. LabCorp's June 4, 2019 SEC filing does not indicate whether it ever contacted AMCA about the issue at any point prior to that week.

Bio-Reference

21. Bio-Reference maintains a network of hundreds of patient service centers that perform a variety of medical tests.

22. On June 3, 2019, Bio-Reference admitted in an SEC filing that its patients had been the victims of a data breach:

> On or around June 3, 2019, BioReference Laboratories, Inc. ("BioReference"), a subsidiary of OPKO Health Inc. (the "Company"), was notified by Retrieval-Masters Creditors Bureau, Inc. d/b/a American Medical Collection Agency ("AMCA") about unauthorized activity on AMCA's web payment page (the "AMCA Incident"). AMCA is an external collection agency that has been used in the past by BioReference and other healthcare companies. According to AMCA, the unauthorized activity occurred between August 1, 2018, and March 30, 2019. AMCA has advised BioReference that data for approximately 422,600 patients for whom BioReference performed testing was stored in the affected AMCA system. AMCA advised that AMCA's affected system includes information provided by BioReference that may have included patient name, date of birth, address, phone, date of service, provider, and balance information. In addition, the affected AMCA system also included credit card information, bank account information (but no passwords or security questions) and email addresses that were provided by the consumer to AMCA. AMCA has advised BioReference that no Social Security Numbers were compromised, and BioReference provided no laboratory results or diagnostic information to AMCA. BioReference has not been able to verify the accuracy of the information received from AMCA.

23. Bio-Reference's SEC filing does not reference any communications regarding the Data Breach dated prior to June 3, 2019.

Clinical Pathology Laboratories, Inc.

24. CPL offers laboratory services to patients at over 200 locations in eight states.

25. On July 12, 2019, CPL issued a press release disclosing that it had been informed by AMCA of a data security incident involving the AMCA payment website.

26. That press release further disclosed the following:

> According to AMCA, on March 21, 2019, AMCA became aware of facts indicating there had been a data security incident. After conducting an 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. However, at the time of AMCA's initial notification, AMCA did not provide CPL with enough information for CPL to identify potentially affected patients or confirm the nature of patient information potentially involved in the incident, and CPL's investigation is on-going. Based 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.

27. Although CPL claims to have known 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.

General Allegations

28. Defendants' common vendor, AMCA, allowed hackers to access Plaintiffs' and other Class Members' Sensitive Information for at least seven months. Defendants and AMCA collectively did nothing to let the victims know about the Data Breach for nearly a year after it began.

29. On February 28, 2019, analysts at Gemini Advisory disclosed a data breach at AMCA which had 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.

American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory, Databreaches.net (May 10, 2019), https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/ (lasted visited Aug. 8, 2019). Gemini Advisory's "research revealed that the exposure window lasted for at least seven months beginning in September, 2018." *Id.* AMCA refused to answer questions from Gemini Advisory at the time. *Id.*

30. Although Defendants should have known of the Data Breach no later than March 2019, and although AMCA knew of it far earlier than that, Defendants took no steps to notify patients whose information was affected until June 3, 2019.

31. Defendants had obligations, 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.

32. Defendants' data security obligations 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.

33. 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 Class's 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

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

35. 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.[1] 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.

36. 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."[2]

37. 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.

38. 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*

---

1 *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 June 4, 2019).

2 *Id*. at 2, 9.

continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[3]

39. 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.[4]

40. 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.

41. 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.[5]

---

[3] *Id*. at 29 (emphasis added).

[4] *See Federal Trade Commission,* Warning Signs of Identify Theft, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited June 4, 2019).

[5] *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 June 4, 2019).

42. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole. 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."[6] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

CLASS ALLEGATIONS

43. 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 the Class defined as follows**:**

> All persons in the United States whose Sensitive Information was maintained on the AMCA systems that were compromised as a result of the breaches announced by Defendants in June and July of 2019.

44. The Class is so numerous that joinder of all members is impracticable. On information and belief, the Class has more than 1,000 members. Moreover, the disposition of the claims of the Class in a single action will provide substantial benefits to all parties and the Court.

45. 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 complied with all applicable legal requirements;

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

---

[6] *See* Study; Few Aware of Medical Identity Theft Risk, Claims Journal, http://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited June 4, 2019).

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.

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

47. Plaintiffs will fairly and adequately protect the interests of the Class. 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 Class 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 Class.

48. 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.

49. A class action is the superior method for the fair and efficient adjudication of this controversy. Class Members' interests in individually controlling the prosecution of separate actions are 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.

50. 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 COUNT
Negligence
Brought by All Plaintiffs on Behalf of Class Members

51. Plaintiffs reallege and incorporate by reference paragraphs 1-50 as if fully set forth herein.

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

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

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

55. Defendants owed a duty of care to Plaintiffs because they collected and stored Plaintiffs' and the Class Members' Sensitive Information and they were foreseeable and probable victims of any inadequate security related policies and practices. Defendants had a common law

duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of the Plaintiffs and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they would be harmed in the future if Defendants did not protect Plaintiffs' and Class Members' information from hackers.

56. Defendants' duties also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of Defendants' duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

57. Each Defendant acknowledged its responsibility to keep customer information secure:

a. Quest acknowledged the need to keep this information secure and stated that "our contractors to whom we may provide such information for the limited purpose of providing services to us and who are obligated to keep the information confidential." Despite this acknowledgment, Quest has not reached out to its customers who had their data breached despite having superior knowledge and being in a position to inform its customers that their data had been hacked. The failure to comply with its Notice of Privacy Practices is just as stark. Quest did not "maintain the privacy" of protected health information, despite acknowledging their legal requirement to do so.

b. LabCorp likewise states in its Privacy Policy that it "contractually require[s] [its] third-party vendors and contractors to comply with strict standards regarding security and confidentiality."

c. Bio-Reference's privacy policy states that it "maintain[s] reasonable security measures to safeguard personal data from loss, interference, misuse, unauthorized access, disclosure, alteration or destruction."

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

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

60. Defendants breached these duties in failing to take reasonable measures or to implement reasonable policies and procedures to prevent the unauthorized access to the Sensitive Information of Plaintiffs.

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

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

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

SECOND COUNT
Negligence *Per Se*
Brought by All Plaintiffs on Behalf of Class Members

64. Plaintiffs reallege and incorporate by reference paragraphs 1-50 as if fully set forth herein.

65. Section 5 of the FTC Act prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Equifax of failing to use reasonable measures to protect personal information. This, along with various FTC publications and orders, also form the basis of Defendants' duty to Plaintiffs and the Class.

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

67. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect personal information and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of personal information it obtained and stored and the foreseeable consequences of a data breach.

68. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

69. Class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

70. Moreover, the harm that has occurred is the type of harm the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses

which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the Class.

71. As a direct and proximate result of Equifax's negligence, Plaintiffs and Class Members have been injured as described herein and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD COUNT
Breach of Contract
Brought by All Plaintiffs on Behalf of Class Members

72. Plaintiffs reallege and incorporate by reference paragraphs 1-50 as if fully set forth herein.

73. Defendants promised to Plaintiff and Class Members, through their privacy policies and its contracts with Class Members, that they would safeguard Plaintiff's and Class Members' Sensitive Information. In exchange for that and other promises made by Defendants, Plaintiffs and Class Members agreed to pay Defendants for medical treatment procedures.

74. Each Defendant's Privacy Policy indicates that they agreed to properly maintain Plaintiff's and Class Members' Sensitive Information, enact safeguards to protect the data, and limit access to the Sensitive Information.

75. Defendants breached their promises by failing to safeguard Plaintiff's and Cass Members' Sensitive Information, failing to detect the data breach, and failing to notify Plaintiff and Class Members in a timely fashion of the data breach.

76. Plaintiff and Class Members have performed all, or substantially all, of the obligations imposed on them under the Privacy Policy and their contracts with Defendants.

77. Plaintiff and Class Members have been damaged as a result of Defendants' breach of their promises.

FOURTH COUNT
Breach of Implied Contract
Brought by All Plaintiffs on Behalf of Class Members

78. Plaintiffs reallege and incorporate by reference paragraphs 1-50 as if fully set forth herein.

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.

FIFTH COUNT

Violation of New York General Business Law § 349

Brought by Plaintiffs Brian Levy and Hannah Weiss on Behalf of New York Class Members

85. Plaintiffs Brian Levy and Hannah Weiss (referred to as "Plaintiffs" in this Count) reallege and incorporate paragraphs 1-50 as if fully set forth herein.

86. 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 from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Defendants failed to take proper action following known security risks and prior cybersecurity incidents, which was a 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).

87. 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.

88. 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, which outweighed any benefits to consumers or to competition.

89. 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-referenced unfair practices and deceptive acts were negligent, knowing and willful.

90. 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. *Id*.

91. 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.

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

SIXTH COUNT
Violation of the Florida Deceptive and Unfair Trade Practices Act, § 501.201, *et seq.*, Fla. Stat. ("FDUTPA")
Brought by Plaintiff Naomi Shapiro on Behalf of Florida Class Members

93. Plaintiff Naomi Shapiro (referred to as "Plaintiff" in this Count) realleges and incorporates paragraphs 1-50 as if fully set forth herein.

94. Plaintiffs is a "consumer" who used her credit cards to make payments to Defendants. *See* § 501.203(7), Fla. Stat.

95. FDUTPA prohibits "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." § 501.204, Fla. Stat.

96. Defendants, by failing to inform consumers (including Plaintiff and Class Members) of its unsecure, non-compliant, and otherwise insufficient data and information security practices, advertised, sold, serviced, and otherwise induced those consumers to purchase goods and services from Defendants.

97. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' Sensitive Information, and that the risk of a data breach was highly likely.

98. Defendants should have disclosed this information regarding its computer systems and data security practices because Defendants were in a superior position to know the true facts related to its defective data security.

99. Florida law requires notification of data breaches upon identification. Upon information and belief, Defendants identified the Data Breach as early as March 2019, but only notified consumers in June and July of 2019, and therefore left those consumers at risk for the months in between discovery and notification.

100. Defendants' failures constitute false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding the security of its network and aggregation of Sensitive Information.

101. The representations upon which consumers (including Plaintiff and Class Members) relied were material representations (e.g., as to Defendants' adequate protection of Sensitive Information), and consumers (including Plaintiff and Class Members) relied on those representations to their detriment.

102. Defendants employed these false representations to promote the sale of a consumer good or service, which Plaintiff and Class Members purchased.

103. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts or practices, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and damages as prescribed by § 501.211(2), Fla. Stat., including attorneys' fees.

WHEREFORE, Plaintiffs and Class Members demand judgment as follows:

A. Certification of the action as a Class Action pursuant to Federal Rule of Civil Procedure 23, and appointment of Plaintiffs as Class Representatives and their counsel of record as Class Counsel;

B. That acts alleged herein be adjudged and decreed to constitute negligence and amount to violations of HIPAA, and the consumer protection laws of New York, Florida, and other states;

C. A judgment against Defendants for the damages sustained by Plaintiffs and the Class defined herein, and for any additional damages, penalties, and other monetary relief provided by applicable law;

D. By awarding Plaintiffs and Class Members pre-judgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of the Complaint in this action;

E. The costs of this suit, including reasonable attorney fees; and

F. Such other and further relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs, individually and on behalf of all those similarly situated, hereby requests a jury trial, pursuant to Federal Rule of Civil Procedure 38, on any and all claims so triable.

Dated: August 9, 2019

/s/ James E. Cecchi

James E. Cecchi
Lindsey H. Taylor
Caroline F. Bartlett
CARELLA BYRNE CECCHI OLSTEIN
BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
(973) 994-1700
jcecchi@carellabyrne.com
ltaylor@carellabyrne.com
cbartlett@carellabyrne.com

Linda P. Nussbaum
Bart D. Cohen
NUSSBAUM LAW GROUP, P.C.
1211 Avenue of the Americas, 40th Floor
New York, NY 10036-8718
(917) 438-9189
lnussbaum@nussbaumpc.com
bcohen@nussbaumpc.com

Jason L. Lichtman
Sean A. Petterson
LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY 10013
(212) 355-9500
jlichtman@lchb.com
spetterson@lchb.com

Michael W. Sobol
LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111
(415.) 956-1000
msobol@lchb.com

Christopher A. Seeger
Parvin Aminolroaya
SEEGER WEISS LLP
55 Challenger Road, 6th Floor
Ridgefield Park, NJ 07660
(973) 639-9100

cseeger@seegerweiss.com
paminolroaya@seegerweiss.com

Paul J. Geller
Stuart A. Davidson
ROBBINS GELLER RUDMAN & DOWD LLP
120 East Palmetto Park Road
Suite 500
Boca Raton, FL 33432
(561) 750-3000
pgeller@rgrdlaw.com
sdavidson@rgrdlaw.com

Samuel H. Rudman
Mark S. Reich
William J. Geddish
ROBBINS GELLER RUDMAN & DOWD LLP
58 S. Service Road, Suite 200
Melville, NY 11747
(631) 367-7100
srudman@rgrdlaw.com
mreich@rgrdlaw.com
wgeddish@rgrdlaw.com

Adam J. Levitt
Amy E. Keller
DICELLO LEVITT GUTZLER LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, IL 60602
(312) 214-7900
alevitt@dicellolevitt.com
akeller@dicellolevitt.com

Adam Frankel
GREENWICH LEGAL ASSOCIATES, LLC
881 Lake Avenue
Greenwich, CT 06831
(203) 622-6001
adam@grwlegal.com

Counsel for Plaintiffs and the Proposed Class