Exhibit C11

UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

GINA ALLENDE and MORGAN OTTMANN, Individually and on Behalf of All Others Similarly Situated, Plaintiffs, v. LABORATORY CORPORATION OF AMERICA, LABORATORY CORPORATION OF AMERICA HOLDINGS, QUEST DIAGNOSTICS INCORPORATED, and OPTUM360 SERVICES, INC., Defendants.	Case No.: **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

INTRODUCTION

1. This class action seeks redress for negligence because Defendants did not implement and maintain reasonable security measures over consumers' sensitive personal information, financial information, and health information.

JURISDICTION AND VENUE

2. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $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 York, and the wrongful acts alleged in this Complaint were committed in New York, 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 Plaintiff's claims occurred in this District,

and 28 U.S.C. § 1391(d) because the transactions giving rise to the claims occurred in Westchester County, New York; and (2) 28 U.S.C. § 1391(b)(3) in that Defendants are subject to personal jurisdiction in this District.

PARTIES

5. Plaintiff Gina Allende is a citizen of the State of Wisconsin who resides in Milwaukee County.

6. Plaintiff Morgan Ottmann is a citizen of the State of Wisconsin who resides in Milwaukee County.

7. Defendant Laboratory Corporation of America ("LCA") is a foreign corporation with principal offices located at 358 South Main Street, Burlington, North Carolina 27215.

8. Defendant Laboratory Corporation of America Holdings ("LCA Holdings") is a foreign corporation with its principal offices located at 358 South Main Street, Burlington, North Carolina 27215.

9. LCA is a wholly owned subsidiary of LCA Holdings.

10. Defendant Quest Diagnostics Incorporated ("Quest") is a Delaware corporation with its principal place of business at 500 Plaza Drive, Secaucus, New Jersey 07094.

11. On information and belief, Defendant Optum360 Services, Inc. ("Optum360") is a Delaware corporation with its principal place of business at 11000 Optum Circle, Eden Prairie, Minnesota 55344.

FACTS

LCA

12. LCA offers a suite of clinical and diagnostic services, serving customers ranging from managed care organizations, biopharmaceutical companies, governmental agencies,

physicians and other healthcare providers, hospitals and health systems, employers, patients and consumers, contract research organizations, and independent clinical laboratories.

13. LCA's website boasts that LCA employs nearly 61,000 employees worldwide, provides diagnostic, drug development and technology-enabled solutions for more than 120 million patient encounters per year, and supports clinical trial activity in approximately 100 countries.

14. LCA is a publicly traded company, and is listed on the New York Stock Exchange under the ticker symbol LH.

15. In the course of providing its services to consumers, LCA acquires consumers' personal and financial information — including consumers' names, addresses, telephone numbers, email addresses, dates of medical services, medical service providers, medical debt balances, and credit card and bank account information ("the Personal Information").

16. In the course of providing its services to consumers, LCA uses the Personal Information to bill consumers for servicers.

17. When consumers find themselves unable to timely pay LCA, LCA typically places consumers' accounts with RMCB, who acts as a third-party collection agency and collects these debts on LCA's behalf.

18. LCA touts its security and industry and regulatory certifications in order to engender trust with potential clients.

19. LCA's website has a webpage dedicated entirely to assuring patients and consumers that their personal and financial information will be secure and private. *See,* https://www.labcorp.com/hipaa-privacy/web-privacy-policy (last accessed: June 11, 2019).

20. LCA's website boasts:

> **How does LabCorp protect the security of your information?**
>
> Financial information and payment data, including credit card numbers, that you provide to us via the LabCorp internet bill payment link is encrypted by using secure socket layer (SSL) encryption technology, which employs a 128-bit encryption system. This information may be accessed only by LabCorp employees who maintain password and job-required access rights, and third party vendors who support LabCorp's billing operations. Additionally, LabCorp maintains all personal patient data within the LabCorp information system (IS) firewalls that operate on separate LabCorp mainframes/servers. The general public may not access these mainframes/servers.

https://www.labcorp.com/hipaa-privacy/web-privacy-policy (last accessed: June 11, 2019).

Quest

21. 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.

22. Quest promises patients that it will keep their Sensitive Information confidential, assuring patients that it is "committed to protecting the privacy of your identifiable health information." http://questdiagnostics.com/home/privacy-policy/notice-privacypractices.html (last visited June 3, 2019).

23. In its Notice of Privacy Practices, Quest acknowledges that it is subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). *Id.*

24. Quest informs patients: "We may provide your PHI [(Private Health Information)] to other companies or individuals that need the information to provide services to us. These other entities, known as 'business associates,' are required to maintain the privacy and security of PHI." *Id.*

The RMCB Data Breach and LCA's and Quest's Insufficient Reactions

25. Non-party Retrieval Masters Creditors Bureau, Inc. ("RMCB") is a foreign corporation with principal offices located at 4 Westchester Plaza, Suite 110, Elmsford, New York 10523.

26. RMCB does business under the fictitious or trade name "American Medical Collection Agency."

27. As a result of RMCB's conduct described below, RMCB filed a petition for Chapter 11 protection in the Southern District of New York on June 17, 2019. In re Retrieval-Masters Creditors Bureau, Inc., No. 19-23185-rdd (S.D.N.Y. Bkr. *filed* June 17, 2019). RMCB is not named as a party to this action due to the bankruptcy filing.

28. 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.

29. 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.

30. Quest apparently allowed hackers to access Plaintiff's and other Class Members' Sensitive Information for some seven months, and did nothing to let the victims know about the Data Breach for nearly a year after it began.

31. Although Quest knew of the Data Breach at least as of May 14, 2019, and although AMCA knew of it even earlier, neither took any steps to notify patients whose information was affected until June 3, 2019, at which point Quest only did so through an SEC filing.

32. Quest and RMCB were in possession of Sensitive Information relating to Plaintiff Ottmann at the time of the Data Breach.

33. Upon information and belief, hackers had access to Sensitive Information relating to Plaintiff Ottmann at the time of the Data Breach.

34. Similarly, on June 4, 2019, LCA announced that it was notified by RMCB that unauthorized users had access to RMCB's system that contained information that RMCB had received from various entities, including LCA and information that RMCB collected itself.

35. LCA announced that it had referred patient balances to RMCB after LCA's direct collection efforts were unsuccessful.

36. LCA further announced that RMCB notified LCA that there was a security incident involving unauthorized activity on an RMCB information technology system between August 1, 2018 and March 30, 2019.

37. LCA further announced that the affected system contained information provided by LCA and patients, including patients' and consumers' Personal Information.

38. LCA further announced that the Data Breach included the Personal Information of some 7.7 million patients, and included, at a minimum:

- Patients' first and last names;
- Patients' dates of birth;
- Patients' addresses;
- Patients' phone numbers;

- Patients' dates of medical service;
- Patients' medical providers;
- Patients' medical debt balances;
- Patients' credit card information; and
- Patients' bank account information

39. LCA further announced that LCA did not provide consumers' ordered test, laboratory results, or clinical information to RMCB, and that RMCB claimed to LCA that RMCB does not store or maintain patients' social security numbers and insurance information.

40. By referencing LCA and RMCB's representations, Plaintiffs do not intend to endorse the representations, nor concede in any way that the representations made therein are accurate or true. They are referenced merely to show that the statements were made and Plaintiffs received them. Further, unlike patients' ordered test, laboratory results, and clinical information, it appears that LCA did, in fact, provide patients' social security numbers and insurance information to RMCB.

41. LCA and RMCB were in possession of Sensitive Information relating to Plaintiffs Allende at the time of the Data Breach.

42. Upon information and belief, hackers had access to Sensitive Information relating to Plaintiff Allende at the time of the Data Breach.

43. As a result of RMCB's failure to implement and maintain reasonable security measures to protect Personal Information from unauthorized access—and both LCA's and Quest's respective failures to ensure that RMCB was implementing and maintaining reasonable security measures to protect consumers' Personal Information—the Personal Information of Plaintiffs and

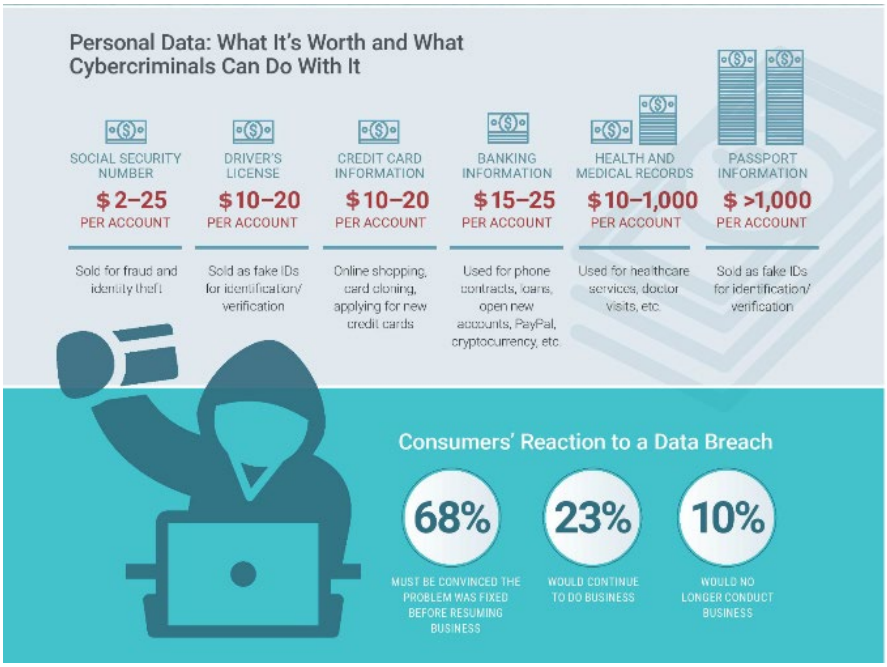
other Class members was accessed and viewed by unauthorized individuals at some point between August 1, 2018 and March 30, 2019, if not earlier ("the Data Breach").

44. Upon information and belief, as a result of the Data Breach, Plaintiffs' and the other Class members' Personal Information, and perhaps more information, is now in the hands of unknown persons who intend to use it for criminal or nefarious purposes.

45. Upon information and belief, the unauthorized persons will sell the Personal Information to exploit and injure Plaintiffs and the other Class members, to commit identity theft and identity fraud, and commit other acts injurious and detrimental to Plaintiffs and the other Class members.

46. It is widely understood that there is a "black market" for consumers' Personal Information like the Personal Information that was obtained in the Data Breach.

47. Indeed, recent studies show that credit card information and banking information can fetch up to $20-25 per account, and health and medical records can fetch up to $1,000 per account:



Megan Leonhardt, "Here's How Much Money Hackers Get for Your Social Security Number and Other Info on the Black Market," CNBC (publ. Aug. 22, 2018) (available at: https://www.cnbc.com/2018/08/22/how-much-hackers-get-for-social-security-numbers-on-the-black-market.html) (last accessed: June 11, 2019).

48. Plaintiffs and the other Class members had their Personal Information entrusted in the wrong hands. Despite LCA's and Quest's assurances and representations, LCA and Quest engaged RMCB to collect consumer debts without assuring that RMCB implemented and maintained reasonable data security practices in accordance with its representations and the obligations it owes under the law.

49. Upon information and belief, Plaintiffs and the other Class members' Personal Information was accessed, viewed, downloaded, acquired, and stolen by unauthorized persons from RMBC's website. The letter leaves open the possibility that other information was also compromised.

50. LCA's general announcement is insufficient to comply with its and RMCB's obligations to provide adequate and timely notification of the Data Breach under the law. LCA and RMCB awaited a sophisticated and extensive forensic investigation when timely notification of the Data Breach was of the essence. LCA and RMCB kept the incident secret from Plaintiffs and the other Class members for at least 2 months, and possibly almost a year. Data thieves had at least 2 months from the alleged beginning of the Data Breach until notification to perpetrate fraud using the Personal Information with no victim even being aware of the threat.

51. LCA's general announcement identified that there were 7.7 million LCA patients affected, and that at least 200,000 of these patients had their credit card and bank account

information breached. Upon information and belief, many of these patients reside in the state of Wisconsin.

52. Further, the Health Information Portability and Accountability Act of 1996 ("HIPAA") impose additional obligations on Defendants to ensure that patients' Personal Information remains confidential, and to prevent the unauthorized disclosure of patients' Personal Information. *See, e.g.,* 45 C.F.R. § 164 *et seq.* (governing security and privacy of protected health information).

53. It did not take long for misinformation to spread online. Theories abound about the actual nature of the breach, whether it is legitimate or not, and whether other entities also disclosed consumers' Personal Information. This misinformation filling the void of Defendants' silence allows for phishing and other scams to seize advantage of those already victimized by the Data Breach.

54. In a somewhat ironic twist, LCA has not only attempted to distance itself and absolve itself of liability for the Data Breach by suggesting that only RMCB is at fault, and RMCB is the responsible entity, but has also attempted to redirect the blame for the disclosure of patients' Personal Information back to the patients themselves, advising patients that RMCB would not have had their information in the first place, but for the fact that "LabCorp's own direct collection efforts were unsuccessful." https://www.labcorp.com/AMCA-data-security-incident (last accessed: June 11, 2019).

55. As a direct and foreseeable result of Defendants' failures, Plaintiffs and the other Class members' Personal Information was placed onto unsecure and vulnerable online locations. At a minimum, sensitive personal, financial, and medical information (and perhaps more) was

accessed, viewed, obtained, downloaded, and is now in the hands of unknown individuals intent on using the information to harm Plaintiffs and the other Class members.

Data Breaches Lead to Identity Theft

56. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.[1]

57. The Federal Trade Commission ("FTC") cautions that identity theft wreaks havoc on consumers' finances, credit history and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[2]

58. Personal 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 a number of years.[3] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen private information directly on various Internet websites, making the information publicly available.

---

[1] *See Victims of Identity Theft*, 2014, DOJ, at 1 (2015), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 19, 2018).

[2] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[3] Companies, in fact, also recognize Personal Information as an extremely valuable commodity akin to a form of personal property. *See* John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PERSONAL INFORMATION") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

59. In fact, "[a] quarter of consumers that received data breach letters [in 2012] wound up becoming a victim of identity fraud."[4]

The Monetary Value of Privacy Protections and Personal Information

60. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[5]

61. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[6]

62. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[7]

---

[4] *One in Four that Receive Data Breach Letters Affected By Identity Theft*, available at https://blog.kaspersky.com/data-breach-letters-affected-by-identity-theft/ (last visited July 19, 2018).

[5] Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited July 19, 2018).

[6] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited July 19, 2018).

[7] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited July 19, 2018).

63. Recognizing the high value that consumers place on their Personal Information, many companies now offer consumers an opportunity to sell this information. The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their personal information.[8] This business has created a new market for the sale and purchase of this valuable data.[9]

64. Consumers place a high value not only on their personal information, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349."[10]

65. The value of Plaintiff's and Class members' Personal Information on the black market is substantial. By way of the Data Breach, Defendants deprived Plaintiff and Class members of the substantial value of their Personal Information. Rather than have an unknown third party realize the value of her Personal Information, Plaintiff would choose to realize that value himself.

Damages Sustained by Plaintiffs and the Other Class Members

66. Plaintiffs and other members of the Class have suffered injury and damages, including, but not limited to: (i) an increased risk of identity theft and identity fraud;

---

[8] Steve Lohr, *You Want My Personal Data? Reward Me for It, The New York Times*, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited July 19, 2018).

[9] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited July 19, 2018).

[10] *See Victims of Identity Theft*, 2014, DOJ, at 1 (2015), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 19, 2018).

(ii) improper disclosure of their Personal Information, which is now in the hands of criminals; (iii) the value of their time spent mitigating the increased risk of identity theft and identity fraud; (iv) the value of their time and expenses associated with mitigation, remediation, and sorting out the risk of fraud and actual instances of fraud; and (v) deprivation of the value of their Personal Information, for which there is a well-established national and international market.

67. Plaintiffs and the other Class members have suffered and will continue to suffer additional damages based on the opportunity cost and value of time that Plaintiffs and the other Class members have been forced to expend and must expend in the future to monitor their financial accounts and credit files as a result of the Data Breach.

COUNT I – NEGLIGENCE

68. Plaintiffs incorporate by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

69. Defendants owed to Plaintiffs and the other Class members a duty to exercise reasonable care in handling and using the Personal Information in its custody, including:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Personal Information in its possession;

b. to protect Personal Information in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices and the practices and certifications represented on its website which it voluntarily undertook duties to implement; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly and sufficiently notifying Plaintiffs and the other members of the Class of the Data Breach.

70. Defendants, purported experts in legal compliance, knew or should have known the risks of collecting and storing Personal Information and the importance of maintaining secure systems. Defendants knew of the many breaches that targeted other entities in the years preceding the Data Breach.

71. Given the nature of Defendants' business collecting and maintaining consumers' sensitive personal, medical, and financial information, the sensitivity and value of the information it maintains, and the resources at its disposal, Defendants' should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

72. Defendants owed these duties to Plaintiffs and the other Class members because Plaintiffs and the other Class members are a well-defined, foreseeable, and probable class of individuals whom Defendants should have been aware could be injured by Defendants' inadequate security protocols. Defendants actively solicited Plaintiffs and the other Class members' Personal Information, and used this information for Defendants' profit.

73. Further, under Wis. Stat. § 134.98, Defendant owed to Plaintiffs and the other Class members a duty to notify them within a reasonable timeframe of any breach to the security of their personal information.

74. Defendants breached the duties owed to Plaintiffs and Class members in several ways, including:

a. by failing to implement, maintain, and ensure adequate security systems, protocols and practices sufficient to protect Personal Information and thereby creating a foreseeable, unreasonable risk of harm;

b. by failing to comply with the minimum industry data security standards and its own assurances of superior data security standards;

c. by negligently performing voluntary undertakings to secure and protect the Personal Information it solicited and maintained; and

d. by failing to timely and sufficiently discover and disclose to consumers that their Personal Information had been improperly acquired or accessed, and providing misleading and unfounded suggestions that their information (and by extension their identity) is not in the immediate peril it is in fact in.

e. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiffs and the other Class members, their Personal Information would not have been compromised.

75. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendants' negligent conduct. Plaintiffs and the other Class members have suffered actual damages including improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

76. Plaintiffs' and the other Class members' injuries were proximately caused by Defendants' violations of the common law duties enumerated above, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT II - INTENTIONAL MISREPRESENTATION

77. Plaintiffs incorporate by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

78. Defendants knowingly made false and deceptive representations regarding their data security practices and policies, in their privacy statement and elsewhere, including enumerating specific uses and ways in which the information could be shared.

79. Defendants additionally knowingly made false and deceptive statements to cover up and conceal the Data Breach through knowing misrepresentations and omissions of material fact. Defendant knowingly misrepresented the ransom paid to the hackers, and falsely labeling it a bug bounty. Defendant omitted the material fact that the ransom was actually paid to hackers who had executed the Data Breach.

80. These knowing misrepresentations were intended to conceal and delay the notification of and the investigation into the Data Breach for more than a year in order to induce the public to enter into a contract for Defendant's services and/or increase consumption of Defendant's services.

81. As a result of Defendants false statements, Plaintiff and the other Class members continued to use Defendants' services and have suffered additional pecuniary loss, including improper disclosure of their Sensitive Information, lost benefit of the bargain, lost value of their Sensitive Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT III - BREACH OF CONTRACT

82. Plaintiffs incorporate by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

83. Defendants entered into contracts with Plaintiffs and the other Class members, which includes terms covering privacy and limiting the use and sharing of Plaintiffs' and the other Class members' personal information.

84. Plaintiffs and the other Class members bargained for an adequate level of security and reasonable care with respect to the use, storage, and sharing of their personal information.

85. Plaintiffs and the other Class members performed their duties under the agreements.

86. Defendants violated the terms of their respective contracts in the Data Breach by sharing Plaintiffs' and the other Class members' personal information for unauthorized purposes, without first obtaining Plaintiffs' or the other Class members' consent or anonymizing and/or aggregating the information in a form which cannot reasonably be used to identify them, and otherwise violating the terms of the contract.

87. Defendants violated the terms of the contract in the Data Breach by failing to take appropriate measures to protect Plaintiffs' and the other Class members' personal information in accordance with its promises and representations. Defendants violated the agreement by failing to comply with applicable laws during the Data Breach regarding the access, correction, and/or deletion of personal data, and notification to affected persons.

88. Plaintiffs and the other Class members have suffered actual damages including improper disclosure of their Sensitive Information, lost benefit of the bargain, lost value of their Sensitive Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT IV - BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

89. Plaintiffs incorporate by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

90. The law implies a covenant of good faith and fair dealing in every contract.

91. Defendants entered into contracts with Plaintiffs and the other Class members, which include terms covering privacy and limiting the use and sharing of Plaintiffs' and the other Class members' personal information.

92. Plaintiffs and the other Class members performed their duties under the agreements.

93. Defendants' unlawful and bad faith conduct, as described above, constitutes a breach of the implied covenant of good faith and fair dealing.

94. Plaintiffs and the other Class members have suffered actual damages including improper disclosure of their Sensitive Information, lost benefit of the bargain, lost value of their Sensitive Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT V - VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349

95. Plaintiffs incorporate by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

96. 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-a(2).

97. 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.

98. 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.

99. 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.

100. 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*.

101. 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.

102. 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.

CLASS ALLEGATIONS

103. Plaintiffs bring this action on behalf of two Classes.

104. Class 1 (the "LCA Class") consists of:

> All persons residing in the United States of America whose Personal Information with LCA was held by RMCB during the Data Breach that occurred from at least August 1, 2018 through March 30, 2019. Plaintiff Allende is the designated representative for Class 1. Excluded from the foregoing class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

105. Plaintiffs bring this action on behalf of a subclass of Wisconsin residents, consisting of:

> All persons residing in the State of Wisconsin whose Personal Information with LCA was held by RMCB during the Data Breach that occurred from at least August 1, 2018 through March 30, 2019. Plaintiff Allende is the designated representative

for this subclass. Excluded from the foregoing class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

106. Class 2 (the "Quest Class") consists of:

All persons residing in the United States of America whose Personal Information with Quest was held by RMCB during the Data Breach that occurred from at least August 1, 2018 through March 30, 2019. Plaintiff Ottmann is the designated representative for Class 2. Excluded from the foregoing class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

107. Plaintiffs bring this action on behalf of a subclass of Wisconsin residents, consisting of:

All persons residing in the State of Wisconsin whose Personal Information with Quest was held by RMCB during the Data Breach that occurred from at least August 1, 2018 through March 30, 2019. Plaintiff Ottmann is the designated representative for this subclass. Excluded from the foregoing class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

108. Each Class is so numerous that joinder is impracticable. Upon information and belief, there are at least seven million members of the LCA Class and at least twelve million members of the Quest Class.

109. There are questions of law and fact common to the members of each Class, which common questions predominate over any questions that affect only individual class members. The predominant common questions include:

a. Whether each Defendant had a duty to protect Plaintiffs' and Class members' Personal Information;

b. Whether each Defendant knew or should have known of the susceptibility of their data security systems to a data breach;

c. Whether each Defendant's security measures to protect its systems and consumers' financial information was reasonable in light of the measures recommended by data security experts;

d. Whether each Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether each Defendant's failure to implement adequate data security measures allowed the breach to occur;

f. Whether each Defendant's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in disclosure of the Personal Information of Plaintiffs and Class members;

g. Whether Plaintiffs and Class members are entitled to relief.

110. Plaintiffs' claims are typical of the claims of the Class members. All are based on the same factual and legal theories.

111. Plaintiffs will fairly and adequately represent the interests of the Class members. Plaintiffs have retained counsel experienced in consumer class action cases including data breach litigation.

112. A class action is superior to other alternative methods of adjudicating this dispute. Individual cases are not economically feasible.

JURY DEMAND

113. Plaintiffs hereby demand a trial by jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request that the Court enter judgment in favor of Plaintiffs and the Class and against Defendants for:

(a) actual damages;

(b) statutory damages;

(c) punitive damages;

(d) injunctive relief;

(e) attorneys' fees, litigation expenses and costs of suit; and

(f) such other or further relief as the Court deems proper.

Dated: June 26, 2019

Respectfully submitted,

MONTEVERDE & ASSOCIATES PC

/s/ Juan E. Monteverde

Juan E. Monteverde (JM-8169)
The Empire State Building
350 Fifth Avenue, Suite 4405
New York, NY 10118
Tel:(212) 971-1341
Fax:(212) 202-7880
jmonteverde@monteverdelaw.com

Attorneys for Plaintiffs

OF COUNSEL

ADEMI & O'REILLY, LLP
Shpetim Ademi (SBN 1026973)
John D. Blythin (SBN 1046105)
Denise L. Morris (SBN 1097911)
3620 East Layton Avenue
Cudahy, WI 53110
(414) 482-8000
(414) 482-8001 (fax)
sademi@ademilaw.com
jblythin@ademilaw.com
dmorris@ademilaw.com

Attorneys for Plaintiffs