Exhibit C10

UNITED STATES DISTRICT COURT

IN THE SOUTHERN DISTRICT OF NEW YORK

KAESHA GAYE CAMILIA HENRY, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. AMERICAN MEDICAL COLLECTION AGENCY, INC., LABORATORY CORPORATION OF AMERICA HOLDINGS, QUEST DIAGNOSTICS INCORPORATED, OPTUM360, LLC, BIOREFERENCE LABORATORIES, INC., and DOES 1-50, Defendants.	Case No. 19-CV-5392 **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

Plaintiff Kaesha Gaye Camilia Henry, on behalf of herself and all others similarly situated, through undersigned counsel, hereby alleges the following against Defendants American Medical Collection Agency, Inc. ("AMCA"), Laboratory Corporation of America Holdings ("LabCorp"), Quest Diagnostics Incorporated ("Quest"), Optum360, LLC ("Optum360"), BioReference Laboratories, Inc. ("BioReference"), and Does 1-50 (the "Doe Defendants") (collectively, the "Defendants") as follows:

INTRODUCTION

1. LabCorp, one of the largest medical testing providers in the country, collects private personal, medical, and financial information from its customers in providing its services. LabCorp utilizes AMCA for billing collection services. AMCA obtains and shares LabCorp customers' personal information and is charged with safeguarding private medical, personal, and

financial information.

2. Quest, one of the largest medical testing providers in the country, collects its customers' private medical and financial information in providing its services. Quest contracts with Optum360 for revenue services operations. In turn, Optum360 utilizes AMCA for billing collection services. Optum360 and AMCA obtain and share Quest customers' personal information and are charged with safeguarding private medical, personal, and financial information.

3. BioReference, a subsidiary of OPKO Health, Inc., is a large medical testing provider. BioReference collects private personal, medical, and financial information from its customers in providing its services. BioReference utilizes AMCA for billing collection services. AMCA obtains and shares BioReference customers' personal information and is charged with safeguarding private medical, personal, and financial information.

4. On June 3, 2019, Quest revealed in a press release and securities filing with the U.S. Securities and Exchange Commission ("SEC") that unauthorized parties had access and did access the system run by AMCA for over a seven-month period between August 2018 and March 2019 (the "Data Breach").

5. On the same day, BioReference revealed in a press release and securities filing with the SEC that unauthorized parties had access and did access the system run by AMCA for over the same seven-month period between August 2018 and March 2019.

6. On June 4, 2019, LabCorp revealed to the media and in a securities filing with the SEC that unauthorized parties had access and did access the system run by AMCA for over a seven-month period between August 2018 and March 2019.

7. Quest admitted that Plaintiff's and Class Members' 1) protected health

information ("PHI"), as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 2) personally identifiable information ("PII") – such as mailing address, phone number, email address, date of birth, gender, and other personal information – and 3) financial information – such as credit and debit card numbers and other payment card data – were accessed (collectively, "Personal Information").

8. BioReference admitted that Plaintiff's and Class Members' 1) PII – such as mailing address, phone number, email address, date of birth, date of service and other personal information – and 2) financial information – such as credit card or bank account information – were accessed.

9. Similarly, LabCorp admitted that Plaintiff's and Class Members' 1) PII – such as mailing address, phone number, email address, date of birth, date of service and other personal information – and 2) financial information – such as credit card or bank account information – were accessed.

10. LabCorp further stated that it had referred approximately 7.7 million consumers to AMCA whose Personal Information was stored on the affected systems. LabCorp stated that AMCA is sending notices to approximately 200,000 LabCorp consumers whose information may have been accessed but had not yet received a list of affected consumers or more specific information.

11. Quest admitted that, as of May 31, 2019, AMCA believed that 11.9 million Quest patients had their Personal Information on the affected systems. However, Quest has not verified the accuracy of this information.

12. BioReference stated that approximately 423,000 BioReference patients had their Personal Information on AMCA's affected systems. BioReference further stated that AMCA is

sending notices to approximately 6,600 BioReference consumers whose information may have been accessed but had not yet received a list of affected consumers or more specific information.

13. AMCA allegedly learned about the Data Breach on or around March 20, 2019 through a third-party security compliance firm that works with credit card companies. AMCA does not state which compliance firm notified AMCA. However, AMCA did not inform Quest and Optum360 of the Data Breach until May 14, 2019. Nor is there any indication that AMCA informed LabCorp or BioReference of the Data Breach until LabCorp and BioReference made statements on June 3 and June 4, respectively.

14. But AMCA had been informed of a data breach for approximately 200,000 individuals as early as March 1, 2019 by a third-party company specializing in detecting such breaches. AMCA did not respond to the third-party company.

15. Defendants' failure to protect their information is a breach of their implied contracts with Plaintiff and Class Members. Further, Defendants' failure to protect such information violates their legal duties and consumer protection and privacy laws.

16. LabCorp's widespread failure to safeguard customers' information was directly contrary to its representations that any information shared with contractors was "for the limited purpose of providing services to us and who are obligated to keep information confidential." LabCorp's "Notice of Privacy Practices" explicitly states that it is "required to maintain the privacy of health information that identifies you" and "is committed to the protection of your PHI and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation."

17. Quest's widespread failure to safeguard its customers' information was directly contrary to Quest's representations in its privacy policy that any information shared with

contractors was "for the limited purpose of providing services to us and who are obligated to keep information confidential." Quest's "Notice of Privacy Practices" explicitly states that it is "required by law to maintain the privacy of your PHI."

18. BioReference's widespread failure to safeguard its customers' information was directly contrary to BioReference's representations in its privacy policy that any its contractors would "to take reasonable steps to protect the privacy of your personal data and PHI as required by law and/or contract" and "are directly bound by law and/or contract to protect your information." BioReference's "Notice of Privacy Practices" explicitly states that it is "required by law to protect the privacy of your personal data and PHI."

19. Defendants' failure to maintain reasonable and/or adequate security measures to protect Plaintiff's and Class Members' Personal Information has caused and will continue to cause harm for the indefinite future.

20. Defendants' intentional, willful, reckless, and/or negligent conduct damaged Plaintiff and Class Members.

PARTIES

21. Plaintiff Kaesha Gaye Camilia Henry is an individual residing in Miramar, Florida. She had been a patient at LabCorp prior to or during the relevant period. Based on LabCorp's determination that she had not paid her bill, LabCorp sent Ms. Henry's Personal Information to AMCA for collection purposes during the relevant period. On information and belief, Ms. Henry's Personal Information was compromised in the Data Breach described herein.

22. Defendant American Medical Collection Agency, Inc., also known as Retrieval-Masters Creditors Bureau, Inc., is a New York corporation founded in 1977, with its principal place of business in Elmsford, New York. It purports to be the leading recovery agency for

patient collections.

23. Defendant Laboratory Corporation of America Holdings is a Delaware corporation with its principal place of business in Burlington, North Carolina. It purports to be a "leading global life sciences company … deeply integrated in guiding patient care through its comprehensive clinical laboratory and end-to-end drug development services."[1]

24. Defendant Quest Diagnostics Incorporated is a Delaware corporation with its principal place of business in Secaucus, New Jersey. It purports to be the "world's leading provider of diagnostic information services."[2]

25. Based on information and belief, Defendant Optum360, LLC is a Delaware corporation with its principal place of business in Eden Prairie, Minnesota. It purports to be "a leading information and technology-enabled health services business."[3]

26. Defendant BioReference Laboratories, Inc. is a subsidiary of OPKO Health Inc. Its principal place of business is in Elmwood Park, New Jersey. It purports to be the nation's third-largest clinical laboratory.[4]

27. The true names and/or capacities, whether individual, corporate, partnership, associate or otherwise, of the Defendants herein designated Does 1 to 50 are unknown to

---

[1] LabCorp, *About Us*. *See* https://www.labcorp.com/about-us (last accessed June 6, 2019).
[2] Quest, *Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 For the Fiscal Year Ended December 31, 2018*, filed on Form 10-K. *See* http://ir.questdiagnostics.com/static-files/3ff1c87e-6764-4890-a5f0-b4a803eefb4b (last accessed June 7, 2019), at 1.
[3] Optum360, *Optum and Quest Diagnostics Partner to Help Make the Health System Work Better for Patients, Physicians, Health Plans and Employers* (Sept. 13, 2016). https://www.optum360.com/about/news/optum-quest-diagnostics-partner-help-make-health-system-work-better-for-patients-physicians-health-plans-employers.html (last accessed June 7, 2019).
[4] BioReference, *OPKO Health*. https://www.bioreference.com/about/about-opko-health/ (last accessed June 7, 2019).

Plaintiff at this time who, therefore, sues said Defendants by fictitious names. Plaintiff alleges that each named Defendant herein designated Doe is negligently, willfully, or otherwise legally responsible for the events and happenings herein referred to and proximately caused damages to Plaintiff and Class Members as herein alleged. Plaintiff will seek leave of Court to amend to insert the true names and capacities of such Defendants when they have been ascertained and will further seek leave to join said Defendants in these proceedings.

JURISDICTION AND VENUE

28. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). This lawsuit is a class action with an amount in controversy over $5 million, involving over 100 proposed class members, some of whom are from a different state than Defendants.

29. This Court may exercise personal jurisdiction over Defendants because they do business in and throughout the State of New York, and the wrongful acts alleged herein were committed in New York, among other venues.

30. Venue is proper in this District pursuant to 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, pursuant to 28 U.S.C. § 1391(d) in that a substantial portion of the injury occurred in this District, and pursuant to 28 U.S.C. § 1391(b)(3) in that Defendants are subject to personal jurisdiction in this District.

FACTUAL ALLEGATIONS

I. THE DATA BREACH

A. LabCorp

31. LabCorp is a leading provider of diagnostic, drug development and technology-

enabled solutions.[5] It performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease. LabCorp purports to have nearly 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."[6]

32. LabCorp asks its customers to bring, among other things, photo identification, current health insurance information, and methods of payment where a customer does or does not have insurance that will cover a particular procedure.[7]

33. LabCorp's invoices cover laboratory testing fees only.[8] When certain customers do not pay their invoices within the requested time period, LabCorp will reach out to its contractor, AMCA, who is then responsible for collecting the outstanding balance.

34. On June 4, 2019, LabCorp publicly admitted in a filing with the SEC that:

> In response to questions it has received, LabCorp® (NYSE: LH) announced that it 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

---

[5] LabCorp, *Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 For the Fiscal Year ended December 31, 2018*, on Form 10-K. *See* https://www.sec.gov/Archives/edgar/data/920148/000092014819000033/lh10-k2018.htm (last accessed June 6, 2019), at 4.
[6] *Id.* at 7.
[7] LabCorp, *What to Expect*. https://www.labcorp.com/labs-and-appointments/what-to-expect (last accessed June 6, 2019).
[8] LabCorp, *How to read your LabCorp laboratory bill. See* https://www.labcorp.com/help/patient-help/how-read-your-labcorp-laboratory-bill (last accessed June 6, 2019);.

> bank account information that was provided by the consumer to AMCA (for those who sought to pay their balance). LabCorp provided no ordered test, laboratory results, or diagnostic information to AMCA. AMCA has advised LabCorp that Social Security Numbers and insurance identification information are not stored or maintained for LabCorp consumers.[9]

35. 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.[10]

36. 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.[11]

37. This exposure "lasted for at least seven months beginning September, 2018, and had affected more than 200,000 victims."[12] However, when Gemini Advisory attempted to notify

---

[9] LabCorp, *Current Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 on Form 8-K*, dated June 4, 2019. *See* https://www.sec.gov/Archives/edgar/data/920148/000119312519165091/d757830d8k.htm (last accessed June 6, 2019).

[10] *Id.*

[11] Databreaches.net, *American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory*, at https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/ (last accessed June 6, 2019).

[12] *Id.*

AMCA on March 1, 2019, it received no response.[13]

38. AMCA states that, on March 20, 2019,[14] 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.[15] AMCA did not provide the information of the security compliance firm that notified it of the "security compromise."

39. LabCorp's June 4 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.

B. Quest

40. Quest operates over 2,200 Patient Service Centers and is a leading provider of medical diagnostic testing services.[16] It performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease.

41. Quest asks its customers to bring, among other things, photo identification, current health insurance information, and methods of payment where a customer does or does not have insurance that will cover a particular procedure.[17]

---

[13] *Id.*
[14] *#1262594:BioReference Laboratories Added to AMCA Breach Tally*. *See* https://brica.de/alerts/alert/public/1262594/bioreference-laboratories-added-to-amca-breach-tally/ (last accessed June 7, 2019).
[15] KrebsonSecurity, *LabCorp: 7.7 Million Consumers Hit in Collections Firm Breach* (June 4, 2019). *See* https://krebsonsecurity.com/2019/06/labcorp-7-7m-consumers-hit-in-collections-firm-breach/ (last accessed June 7, 2019).
[16] Quest, *Why Choose Quest Diagnostics for lab testing*. http://newsroom.questdiagnostics.com/index.php?s=30664 (last accessed June 7, 2019).
[17] Quest, *Preparing for a lab test: getting started.* https://www.questdiagnostics.com/home/patients/preparing-for-test/get-started (last accessed June 7, 2019).

42. Quest's invoices cover laboratory testing fees only.[18] When certain customers do not pay their invoices within the requested time period, Quest will reach out to Optum360, who will provide information to AMCA to collect the balance.

43. On June 3, 2019, Quest publicly admitted in a filing with the SEC that:

> On May 14, 2019, American Medical Collection Agency (AMCA), a billing collections vendor, notified Quest Diagnostics Incorporated ("Quest Diagnostics") and Optum360 LLC, Quest Diagnostics' revenue cycle management provider, of potential unauthorized activity on AMCA's web payment page. Quest Diagnostics and Optum360 promptly sought information from AMCA about the incident, including what, if any, information was subject to unauthorized access.[19]

44. Quest further admitted that:

> Although Quest Diagnostics and Optum360 have not yet received detailed or complete information from AMCA about the incident, AMCA has informed Quest Diagnostics and Optum360 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;
>
> - the information on AMCA's affected system included financial information (*e.g.*, credit card numbers and bank account information), medical information and other personal information (*e.g.*, Social Security Numbers);
>
> - as of May 31, 2019, AMCA believes that the number of Quest Diagnostics patients whose information was contained on AMCA's affected system was approximately 11.9 million people; and

[18] Quest, *Frequently Asked Questions: Billing Services*. *See* https://billing.questdiagnostics.com/PatientBilling/PATFaqExternal.action?getLabCode=false&fromLink=doFaq&csrfToken=25HQ-FBM6-YWHB-O014-IU4Z-TE0V-018H-5IFY (last accessed June 7, 2019).

[19] Quest, *Current Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 on Form 8-K*, dated June 3, 2019. *See* http://ir.questdiagnostics.com/static-files/f8e7fcbb-da1e-46bc-bbbb-98d0fe189f87 (last accessed June 7, 2019).

- AMCA has been in contact with law enforcement regarding the incident.

Quest Diagnostics has not been able to verify the accuracy of the information received from AMCA.[20]

45. Quest's June 3 filing does not indicate that there were any communications between AMCA and Quest concerning the Gemini Advisory notification or any other communications concerning the Data Breach at any point until May 14, 2019.

46. Although Quest and Optum360 knew of the Data Breach since at least May 14, 2019, and although AMCA knew of the Data Breach even earlier, neither took any steps to notify patients whose information was affected until June 3.

C. BioReference

47. BioReference has a network of patient service centers that serves its unique brand entities, including GenPath, Laboratorio Buena Salud and GeneDx.[21] It operates hundreds of sites throughout the United States.[22] It performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease.

48. BioReference's invoices cover laboratory testing fees only.[23] When certain customers do not pay their invoices within the requested time period, BioReference will reach out to its contractor, AMCA, who is then responsible for collecting the outstanding balance.

49. On June 3, 2019, BioReference publicly admitted in a SEC filing that:

On or around June 3, 2019, BioReference Laboratories, Inc.

---

[20] *Id.*
[21] BioReference, *Prepare for your visit. See* https://www.bioreference.com/patients/locations-patient-services/prepare-for-your-visit/ (last accessed June 7, 2019).
[22] BioReference, *Find a location. See* https://www.bioreference.com/patients/locations-patient-services/find-a-location/ (last accessed June 7, 2019).
[23] BioReference, *Billing FAQ. See* https://www.bioreference.com/patients/billing/billing-faq/ (last accessed June 7, 2019).

> ("BioReference"), a subsidiary of OPKO Health Inc. (the "Company"), was notified by Retrieval-MastersCreditors 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.[24]

50. BioReference further admitted that:

> AMCA advised BioReference that it is sending notices to approximately 6,600 patients for whom BioReference performed laboratory testing and whose credit card or bankaccount information was stored in AMCA's affected system. AMCA indicated that it will provide these affected patients with more specific information about the AMCA Incident in addition to offering them identity protection and credit monitoring services for 24 months. AMCA has not yet provided BioReference a list of the affected patients or more specific information about them.[25]

51. BioReference's June 3 filing does not indicate that there were any communications between AMCA and BioReference concerning the Gemini Advisory notification or any communications regarding the Data Breach at any point prior to June 3.

---

[24] BioReference, *Current Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 on Form 8-K*, dated June 3, 2019. *See* https://www.opko.com/investors/sec-filings/all-sec-filings/content/0000944809-19-000039/0000944809-19-000039.pdf (last accessed June 7, 2019).

[25] *Id.*

52. Defendants Quest, Optum360, BioReference, and LabCorp have not provided a Notice of Data Breach[26] and have not adequately explained how the Data Breach occurred or why it took a third party to inform them of the Data Breach. Nor have Defendants disclosed the full extent and nature of the Data Breach as AMCA is "continuing to investigate this incident."[27]

53. Although Defendants should have known of the Data Breach not later than March 2019, and although AMCA knew of the breach earlier, neither took any steps to notify patients whose information was affected until at least June 3, and only in SEC filings.

II. DEFENDANTS' PRIVACY PRACTICES

A. LabCorp

54. LabCorp maintains a Notice of Privacy Practices on its website,[28] which provides:

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

55. Its Notice of Privacy Practices further provides that:

> Business Associates - LabCorp may disclose PHI to its business associates to perform certain business functions or provide certain business services to LabCorp. For example, we may use another company to perform billing services on our behalf. All of our business associates are required to maintain the privacy and

[26] BioReference indicates that "AMCA has advised BioReference that AMCA is providing notice to state attorneys general and other state agencies as required by applicable state data breach laws." *See Current Report*.
[27] LabCorp, *Current Report*.
[28] LabCorp, *LabCorp's Notice of Privacy Practices*. *See* https://www.labcorp.com/hipaa-privacy/hipaa-information (last accessed June 6, 2019).

> confidentiality of your PHI. In addition, at the request of your health care providers or health plan, LabCorp may disclose PHI to their business associates for purposes of performing certain business functions or health care services on their behalf. For example, we may disclose PHI to a business associate of Medicare for purposes of medical necessity review and audit.[29]

56. Thus, LabCorp collects and stores consumers' Personal Information, which it provides to its vendors and contractors such as AMCA to further its business. As recipients of such Personal Information, AMCA is "required to maintain the privacy and confidentiality" of such information.

B. Quest

57. Quest maintains a Notice of Privacy Practices on its website,[30] which provides:

> **Our Responsibilities**
>
> Quest Diagnostics is required by law to maintain the privacy of your PHI. We are also required to provide you with this Notice of our legal duties and privacy practices upon request. It describes our legal duties, privacy practices and your patient rights as determined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). We are required to follow the terms of this Notice currently in effect. We are required to notify affected individuals in the event of a breach involving unsecured protected health information….

58. Its Notice of Privacy Practices further provides:

> **Business Associates**
>
> We may provide your PHI 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. For example, we may provide information to companies that assist us with billing of our services. We may also use an outside collection agency to obtain payment when necessary.[31]

[29] *Id.*
[30] Quest, *Notice of Privacy Practices*. *See* https://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html (last accessed June 7, 2019).
[31] *Id.*

59. Accordingly, Quest collects and stores consumers' Personal Information, which it provides to its vendors and contractors such as AMCA to further its business. As recipients of such Personal Information, AMCA is "required to maintain the privacy and security" of such information.

C. BioReference

60. Quest maintains a Notice of Privacy Practices on its website,[32] which provides:

> **Our Commitment to Safeguard Your Personal Data and Protected Health Information.**
>
> 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)….

61. Its Notice of Privacy Practices further provides:

> **Business Associates.** We may disclose the minimum amount of your personal data and PHI necessary to contractors, agents and other business associates who need the information to help us with billing or other business activities related to the services we provide. For example, we may share personal data and PHI with a billing company that helps us obtain payment from your insurer, an attorney or with a quality assurance consultant in order to obtain their advice regarding our operations. If we do disclose your personal data or PHI to a business associate, we will have a written contract with them that requires the business associate and any of its subcontractors to take reasonable steps to protect the privacy of your personal data and PHI as required by law and/or contract. Business associates and their subcontractors are considered to be data processors and, as such, are directly bound by law and/or contract to protect your information….[33]

[32] BioReference, *Notice of Privacy Practices*. *See* https://www.bioreference.com/wp-content/uploads/2019/02/NOPP-BRLI-January-2019.pdf (last accessed June 7, 2019).
[33] *Id.*

62. Thus, BioReference collects and stores consumers' Personal Information, which it provides to its vendors and contractors such as AMCA to further its business. As recipients of such Personal Information, AMCA is required "to take reasonable steps to protect the privacy of your personal data and PHI as required by law and/or contract."

D. AMCA

63. 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."[34]

III. HIPAA

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

65. The above-mentioned rules establish national standards for the protection of PHI that is held or transmitted by a healthcare provider.

66. Defendants had obligations under HIPAA, their promises made to patients like Plaintiff and Class Members, and based on industry standards, to keep the compromised Personal Information confidential and to protect it from unauthorized disclosures. Class Members provided their Personal Information to LabCorp, Quest, and BioReference with the understanding that these Defendants and any business partners to whom LabCorp, Quest, and

[34] AMCA, *An Industry Leader*. *See* http://amcaonline.com/about.php (last accessed June 6, 2019).

BioReference disclosed Personal Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

67. Defendants' security failures demonstrate that they failed to honor their duties and promises under HIPAA, by failing to:

(a) Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

(b) Adequately protect Plaintiff's and the Class's Personal Information;

(c) Ensure the confidentiality and integrity of electronic PHI that Defendants create, receive, maintain, and/or transmit, in violation of 45 C.F.R. § 164.306(a)(1);

(d) Protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. § 164.306(a)(2);

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

(f) Review and modify security measures implemented under HIPAA as needed to ensure protection of electronic PHI, in violation of 45 C.F.R. § 164.306(a)(4);

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

(h) Implement 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);

(i) Implement 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);

(j) Implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed, in violation of 45 C.F.R. § 164.312(d);

(k) Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule, in violation of 45 C.F.R. § 164.316(a);

(l) Train all members of their workforces effectively on the policies and procedures with respect to PHI, in violation of 45 C.F.R. § 164.530(b); and/or

(m) Design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in violation of 45 C.F.R. § 164.530(c).

IV. THE CONSEQUENCES

68. Consumers place value in data privacy and security. However, Defendants failed to take all necessary precautions to secure the Personal Information given to them by consumers.

69. It is well known that customer Personal Information is an invaluable commodity and a frequent target by hackers. However, despite this widespread knowledge and industry alerts regarding other notable data breaches, Defendants failed to take reasonable steps to adequately protect its systems from being breached.

70. According to Javelin Strategy & Research, in 2018 alone, over 14.4 million

individuals have been affected by identity theft, causing $14.7 billion in fraud incident and fraud losses.[35]

71. Defendants are, and at all relevant times have been, aware that the Personal Information they maintain is highly sensitive and could be used for illegal purposes by third parties. Indeed, Defendants acknowledge that customers expect adequate safeguards of their Personal Information.

72. Consumers place a high value not only on their Personal Information, but also on the privacy of that data. That is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[36]

73. As the Federal Trade Commission ("FTC") has pointed out, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[37]

74. This is the case with social security numbers, the "secret sauce" that is "as good as your DNA to hackers."[38] There are long-term consequences to data breach victims whose social security numbers are taken and utilized. However, Plaintiff and Class Members would not be able to obtain a new number unless they become a victim of social security number misuse. And, even then, the Social Security Administration has warned that "a new number probably

---

[35] Javelin Strategy & Research, *Consumers Increasingly Shoulder Burden of Sophisticated Fraud Schemes, According to 2019 Javelin Strategy & Research Study* (Mar. 9, 2019). *See* https://www.javelinstrategy.com/press-release/consumers-increasingly-shoulder-burden-sophisticated-fraud-schemes-according-2019 (last accessed June 6, 2019).

[36] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*. *See* https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf (last visited June 6, 2019).

[37] 17 C.F.R. § 248.201 (2013).

[38] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, KIPLINGER, (Feb. 10, 2015). *See* https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html (last visited Aug. 1, 2018).

won't solve all [] problems … and won't guarantee … a fresh start."[39]

75. PHI is particularly valuable. According to an April 8, 2014 Private Industry Notification by the Federal Bureau of Investigation, cyber criminals selling valuable PHI on the black market at a rate of $50 per record, as compared to $1 for a stolen social security number or credit card number.[40] That is because such records can be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft.

76. In light of the multiple high-profile data breaches targeting companies such as Target, Neiman Marcus, Marriott International, eBay, Anthem, Premera, Equifax, and Yahoo Inc., Defendants are, or reasonably should have been, aware of the importance of safeguarding its customers' Personal Information, as well as of the foreseeable consequences that would occur if their systems were breached.

77. However, Defendants failed to maintain its data security systems in a meaningful way so as to prevent the Data Breach that occurred. Had Defendants maintained their systems and adequately protected them, it could have prevented the Data Breach.

78. In their SEC filing, LabCorp and BioReference announced that AMCA would offer consumers "identity protection and credit monitoring services for 24 months."[41] Quest, however, has not offered consumers any services.[42] Unfortunately, a person whose Personal Information has been compromised may not fully experience the effects of the breach for years

[39] Social Security Admin., *Identity Theft and Your Social Security Number*. *See* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Aug. 1, 2018), at 6-7.
[40] FBI Cyber Division, *(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (Apr. 4, 2014). *See* https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf (last visited June 7, 2019).
[41] *See* BioReference, *Current Report*; *see also* LabCorp, *Current Report*.
[42] *See* Quest, *Current Report*.

to come.[43] Thus, even with such offered services, Plaintiff and Class Members will nonetheless bear the heightened risk of injury for years to come.

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

80. Defendants had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite their obligation to protect such information.

81. The Data Breach was a direct and proximate result of Defendants' failure to: (1) properly safeguard and protect Plaintiff's and Class Members' Personal Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (2) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Personal Information; and (3) protect against reasonably foreseeable threats to the security or integrity of such information.

82. As a direct and proximate result of Defendants' wrongful actions and inaction, Plaintiff and Class Members have suffered injury and damages, including the increased risk of identity theft and identity fraud, improper disclosure of their Personal Information, the time and expense necessary to mitigate, remediate, and sort out the increased risk of identity theft and

[43] U.S. Government Accountability Office, *Personal Information: Data Breaches for Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007); http://www.gao.gov/assets/270/262904.html (last accessed June 6, 2019).

identity fraud, and a deprivation of the value of their Personal Information.

83. In addition, Plaintiff and Class Members maintain and continues to maintain an unqualified interest in ensuring that their Personal Information is secure, remains secure, and is not subject to further misappropriation and theft.

84. Plaintiff and Class Members have suffered and will continue to suffer additional damages based on the opportunity cost and time Plaintiff and Class Members are forced to expend in the future to monitor their financial accounts and credit files as a result of the Data Breach.

CLASS ALLEGATIONS

85. Plaintiff brings a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and on behalf of a Nationwide Class, defined as follows:

> All persons in the United States whose Personal Information was maintained on AMCA's systems and was compromised as a result of the Data Breach.

86. Plaintiff brings a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of herself and on behalf of a Florida Class, defined as follows:

> All persons in Florida whose Personal Information was maintained on AMCA's systems and was compromised as a result of the Data Breach.

87. Excluded from the above classes is: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which Defendants have a controlling interest, and its current or former employees, officers, and directors; (3) counsel for Plaintiff and Defendants; and (4) legal representatives, successors, or assigns of any such excluded persons.

88. The Classes meet all of the criteria required by Federal Rule of Civil Procedure

23(a).

89. **Numerosity:** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, at least approximately 200,000 individuals from across the country had their Personal Information compromised, stolen, and published by the Data Breach. Indeed, Defendants indicate that the Personal Information of over 20 million individuals have been compromised, stolen, and published by the Data Breach. The parties will be able to identify the exact size of the Classes through discovery and Defendants' documents.

90. **Commonality:** Common questions of law and fact exist as to all Class Members. These common questions of law or fact predominate over any questions affecting only individual members of the Class. Common questions include, but are not limited to, the following:

(a) Whether Defendants engaged in the wrongful conduct alleged herein;

(b) Whether Defendants owed a duty to Plaintiff and members of the Classes to adequately protect their Personal Information;

(c) Whether Defendants' data security systems met legal requirements and industry standards;

(d) Whether Plaintiff's and other Class Members' Personal Information was compromised in the Data Breach;

(e) Whether Plaintiff and Class Members have been injured by virtue of Defendants' conduct;

(f) Whether Plaintiff and Class Members are entitled to damages or other relief from Defendants, and if so, in what amounts; and

(g) Whether Class Members are entitled to injunctive and/or declaratory relief.

91. **Typicality:** Plaintiff's claims are typical of the claims of the Classes she seeks to represent, in that the named Plaintiff and all members of the proposed Classes have suffered similar injuries as a result of the wrongful conduct alleged herein. Plaintiff has no interests adverse to the interests of the other members of the Classes.

92. **Adequacy:** Plaintiff will fairly and adequately protect the interests of the Classes and has retained attorneys well experienced in class actions and complex litigation as her counsel, including cases alleging data breach and consumer protection claims.

93. The Classes also satisfy the criteria for certification under Federal Rule of Civil Procedure 23(b). Among other things, Plaintiff avers that the prosecution of separate actions by the individual members of the proposed classes would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendants; that the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; that Defendants has acted or refused to act on grounds that apply generally to the proposed Classes, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed classes as a whole; that questions of law or fact common to the Classes predominate over any questions affecting only individual members and that class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy which is the subject of this action. Plaintiff further states that the interests of judicial economy will be served by concentrating litigation concerning these claims in this Court, and that the management of the Class will not be difficult.

94. Plaintiff also avers that certification of one or more subclasses or issues may be

appropriate for certification under Federal Rule of Civil Procedure 23(c).

95. Plaintiff and other members of the Class have suffered damages as a result of Defendants' unlawful and wrongful conduct. Absent a class action, Defendants' unlawful and improper conduct shall, in large measure, not go remedied. Absent a class action, the members of the Classes will not be able to effectively litigate these claims and will suffer further losses.

CLAIMS FOR RELIEF

COUNT I

NEGLIGENCE

(on behalf of Plaintiff and the Nationwide Class against Defendants)

96. Plaintiff realleges and incorporates by reference all allegations as though fully set forth herein.

97. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

98. Plaintiff and Class Members were required to provide Defendants with their Personal Information. Defendants collected and stores this information, including their names, payment information, dates of birth, addresses, and phone numbers.

99. By collecting and storing this data, and sharing it and using it for commercial gain, Defendants had a duty to Plaintiff and Class Members to safeguard and protect their Personal Information.

100. Defendants assumed a duty of care to use reasonable means to secure and safeguard this Personal Information, to prevent its disclosure, to guard it from theft, and to detect and attempted or actual breach of their systems.

101. Defendants have full knowledge about the sensitivity of Plaintiff and Class Members' Personal Information, as well as the sort of harm that would occur if such Personal

Information was wrongfully disclosed.

102. Defendants have a duty to use ordinary care in activities which harm might be reasonably anticipated in connection with such Personal Information.

103. Defendants' duty of care further arose as a result of the special relationship that existed between Defendants and Class Members as 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 Plaintiff and Class Members resulting from a data breach.

104. Defendants' duty to use reasonable security measures also arise under HIPAA, which requires Defendants 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 constitutes "protected health information" within the meaning of HIPAA.

105. Defendants' duty to use reasonable security measures also arise under Section 5 of the 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 appropriate measures to protect confidential data.

106. Defendants breached their duty of care by failing to secure and safeguard the Personal Information of Plaintiff and Class Members. Defendants negligently stored and/or maintained its data securities systems.

107. Further, Defendants, by and through their negligent actions and/or inactions, breached their duties to Plaintiff and Class Members by failing to design, adopt, implement, control, manage, monitor, and audit their processes, controls, policies, procedures, and protocols

for complying with applicable laws and safeguarding and protecting Plaintiff's and Nationwide Class Members' Personal Information within their possession, custody, and control.

108. Defendants further breached their duty to Plaintiff and Class Members by failing to comply with state and federal laws designed to protect Plaintiff and Class Members from the type of harm they have suffered. Such a breach by Defendants constitutes negligence per se.

109. Plaintiff and Class Members have suffered harm as a result of Defendants' negligence. The loss of control over the compromised Personal Information subjects Plaintiff and each Class Member to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either use of the compromised information, or access to their user accounts.

110. It was reasonably foreseeable in that Defendants knew or should have known that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Personal Information would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such Personal Information, or disseminated it to other parties for their wrongful use and for no lawful purpose.

111. But for Defendants' negligent and wrongful breach of their responsibilities and duties owed to Plaintiff and Class Members, their Personal Information would not have been compromised.

112. As a direct and proximate result of Defendants' wrongful actions, inactions, and omissions, the result Data Breach and the unauthorized release and disclosure of Plaintiff's and Class Members' Personal Information, they have incurred – and will continue to incur – economic damages, and other actual injury and harm for which they are entitled to compensation. Defendants' wrongful actions, inactions, and omissions constitute common law

negligence.

113. Plaintiff and Class Members are entitled to injunctive relief and actual and punitive damages.

COUNT II

BREACH OF IMPLIED CONTRACT

(on behalf of Plaintiff and Class Members against Defendants)

114. Plaintiff realleges and incorporates by reference all allegations as though fully set forth herein.

115. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

116. When Plaintiff and Class Members paid money and provided their Personal 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 were breached and/or compromised.

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

118. Plaintiff and Class Members would not have provided and entrusted their Personal Information to Defendants in the absence of the implied contract between them and Defendants to keep the information secure.

119. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

120. Defendants breached their implied contracts with Plaintiff and the Class by failing to safeguard and protect their Personal Information and by failing to provide timely and accurate notice that their Personal Information was compromised as a result of the Data Breach.

121. As a direct and proximate result of Defendants' breaches of their implied contracts, Plaintiff and the Class sustained actual losses and damages.

COUNT III

VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349

(on behalf of Plaintiff and the Class against Defendants)

122. Plaintiff realleges and incorporates by reference all allegations as though fully set forth herein.

123. Plaintiff brings this claim on behalf of herself and the Nationwide Class.

124. 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 New York General Business Law § 349(a). This includes but is not limited to the following:

(a) Defendants failed to enact adequate privacy and security measures to protect Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was 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 Personal 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 relevant federal and state laws pertaining to the privacy and security of the Personal 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 matter, in violation of the duties imposed by General Business Law § 899-aa(2).

125. As a direct and proximate result of Defendants' practices, Plaintiff and 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 Personal Information.

126. Defendants' unfair and deceptive acts caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid, which outweighs any benefits to consumers or to competition.

127. Defendants knew or should have known that AMCA's computer systems and data security practices were inadequate to safeguard the Personal Information entrusted to it, and that

risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above unfair practices and deceptive acts were negligent, knowing and willful.

128. Plaintiff seeks relief under General Business Law § 349(h), including but not limited to actual damages, treble damages, statutory damages, injunctive relief, and/or attorneys' fees and costs.

COUNT IV

VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT ("FDUTPA"), FLA. STAT. §§ 501.201, *et seq.*

(on behalf of Plaintiff and the Florida Class against Defendants)

129. Plaintiff realleges and incorporates by reference all allegations as though fully set forth herein.

130. Plaintiff brings this claim on behalf of herself and the Florida Class.

131. Plaintiff is a "consumer" who made payments to Defendants. Fla. Stat. § 501.203(7).

132. 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." Fla. Stat. § 501.204.

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

134. Defendants knew or should have known that their systems and data security practices were inadequate to safeguard Plaintiff's and Class Members' Personal Information, and

that the risk of a data breach was highly likely.

135. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the security of their systems.

136. Florida law requires notification of data breaches upon identification. Upon information and belief, AMCA knew of the Data Breach as early as March 1, 2019, but only notified consumers of such on or about May 14, 2019, and therefore left consumers at risk for the months in between discovery and notification.

137. 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 their computer networks and the aggregation of Personal Information.

138. The representations upon which consumers, including Plaintiff and Class Members, relied were material representations and consumers, including Plaintiff and Class Members, relied on those representations to their detriment.

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

140. As a proximate result of Defendants' unfair and deceptive acts and omissions, Plaintiff's and Class Members' Personal Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on her behalf and on behalf of all Class Members, pray for judgment against Defendants as follows:

A. Certification of the proposed Classes, Appointment of Plaintiff a Class

Representative, and Appointment of the undersigned counsel as counsel for the Classes;

B. An award to Plaintiff and the Classes of compensatory, consequential, incidental, and statutory damages, as allowed by law and in an amount determined at trial;

C. An award of equitable, injunctive, and declaratory relief as maybe appropriate;

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

E. An award of pre-judgment and post-judgment interest as prescribed by law; and

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

DEMAND FOR JURY

Plaintiff demands a trial by jury for all issues so triable.

Respectfully submitted,

Dated: June 7, 2019
New York, New York

KAPLAN FOX & KILSHEIMER LLP

/s/ *Laurence D. King*

Laurence D. King (LK7190)
Mario M. Choi (MC8888)
350 Sansome Street, Suite 400
San Francisco, California 94104
Tel.: (415) 772-4700
Fax: (415) 772-4707
lking@kaplanfox.com
mchoi@kaplanfox.com

Frederic S. Fox
Joel B. Strauss
David A. Straite
850 Third Avenue, 14th Floor
New York, New York 10022
Tel.: (212) 687-1980
Fax: (212) 687-7714
ffox@kaplanfox.com

jstrauss@kaplanfox.com
dstraite@kaplanfox.com

THE LAW OFFICES OF ANDRES MONTEJO, ESQ.
Andres Montejo (*pro hac vice* to be filed)
6157 NW 167 Street, Suite F-21
Miami, Florida 33015
Tel: (305) 817-3677
amontejo@andresmontejolaw.com

Counsel for Plaintiff and the Proposed Classes