# Exhibit C7

**THE UNITED STATES DISTRICT COURT**
**FOR THE MIDDLE DISTRICT OF NORTH CAROLINA**

| | |
|---|---|
| JOANN APONTE, PAMELA DRISKELL, LEO GALLAGHER-KOWIT, JEFFREY GRUSHKA, KIMMIE MARTIN, KIM PARROTT, GARY SCHWALL, CATLIN STANFORD, KERRY STEED, TODD STONE, and MEGAN STOREY, individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>LABORATORY CORPORATION OF AMERICA HOLDINGS d/b/a LABCORP; LABORATORY CORPORATION OF AMERICA d/b/a LABCORP; and AMERICAN MEDICAL COLLECTION AGENCY, INC.,<br><br>Defendants. | Case No.: 1:19-cv-824<br><br>**CLASS ACTION COMPLAINT**<br><br>**JURY TRIAL DEMANDED** |

## CLASS ACTION COMPLAINT

1. Plaintiffs[1] individually and on behalf of a class of all persons similarly situated (the "Class" or "Class Members") bring this class action against Defendants Laboratory Corporation of America Holdings d/b/a LabCorp; Laboratory Corporation of America d/b/a LabCorp; and American Medical Collection Agency, Inc. (collectively, "Defendants"), seeking equitable relief and damages as set forth below.

## PRELIMINARY STATEMENT

2. This is a data breach class action on behalf of approximately 19.6 million individuals whose confidential information was accessed by data thieves in a cyber-attack (the "Breach").

[1] "Plaintiffs" refers to the individuals referenced in the caption above and described more fully *infra* paras. 4–8.

3. Plaintiffs bring this class action on behalf of a Nationwide class and individual Subclasses as defined *infra* against Defendants because of their failure to safeguard and protect the confidential information of millions of patients—including financial information (*e.g.*, credit card numbers and bank account information), medical information, personal information (*e.g.*, Social Security Numbers), and other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, "Personal Information")—and their failure to provide timely notice to Plaintiffs and other Class Members of the nature and scope of the Personal Information that was exposed.

## PARTIES

4. Plaintiff Joann Aponte is a resident of Florida who was a patient of the Defendants during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. As a result of the Breach, and Defendants' failure to prevent it, Ms. Aponte will continue to be at a heightened risk for medical fraud, financial fraud, and identity theft along with the attendant damages for years to come.

5. Plaintiff Pamela Driskell is a resident of Alabama who was a patient of the Defendants during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. As a result of the Breach, and Defendants' failure to prevent it, Ms. Driskell will continue to be at a heightened risk for medical fraud, financial fraud, and identity theft along with the attendant damages for years to come.

6. Plaintiff Leo Gallagher-Kowit is a resident of District of Columbia who was a patient of the Defendants during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. As a result of the Breach, and Defendants' failure to prevent it, Mr. Gallagher-Kowit will continue to be at a heightened risk for medical

fraud, financial fraud, and identity theft along with the attendant damages for years to come.

7. Plaintiff Jeffrey Grushka is a resident of Florida who was a patient of the Defendants during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. As a result of the Breach, and Defendants' failure to prevent it, Mr. Grushka will continue to be at a heightened risk for medical fraud, financial fraud, and identity theft along with the attendant damages for years to come.

8. Plaintiff Kimmie Martin is a resident of Georgia who was a patient of the Defendants during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. As a result of the Breach, and Defendants' failure to prevent it, Ms. Martin will continue to be at a heightened risk for medical fraud, financial fraud, and identity theft along with the attendant damages for years to come.

9. Plaintiff Kim Parrott is a resident of Louisiana who was a patient of the Defendants during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. As a result of the Breach, and Defendants' failure to prevent it, Ms. Parrott will continue to be at a heightened risk for medical fraud, financial fraud, and identity theft along with the attendant damages for years to come.

10. Plaintiff Gary Schwall is a resident of North Carolina who was a patient of the Defendants during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. As a result of the Breach, and Defendants' failure to prevent it, Mr. Schwall will continue to be at a heightened risk for medical fraud, financial fraud, and identity theft along with the attendant damages for years to come.

11. Plaintiff Catlin Stanford is a resident of Georgia who was a patient of the Defendants during the relevant time period and subsequently had Personal Information

compromised as a result of the Breach. As a result of the Breach, and Defendants' failure to prevent it, Ms. Stanford will continue to be at a heightened risk for medical fraud, financial fraud, and identity theft along with the attendant damages for years to come.

12. Plaintiff Kerry Steed is a resident of South Carolina who was a patient of the Defendants during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. As a result of the Breach, and Defendants' failure to prevent it, Mr. Steed will continue to be at a heightened risk for medical fraud, financial fraud, and identity theft along with the attendant damages for years to come.

13. Plaintiff Todd Stone is a resident of Florida who was a patient of the Defendants during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. As a result of the Breach, and Defendants' failure to prevent it, Mr. Stone will continue to be at a heightened risk for medical fraud, financial fraud, and identity theft along with the attendant damages for years to come.

14. Plaintiff Megan Storey is a resident of Kentucky who was a patient of the Defendants during the relevant time period and subsequently had Personal Information compromised as a result of the Breach. As a result of the Breach, and Defendants' failure to prevent it, Ms. Storey will continue to be at a heightened risk for medical fraud, financial fraud, and identity theft along with the attendant damages for years to come.

15. Defendant LabCorp[2] operates laboratory locations throughout the United States including within North Carolina. Defendant LabCorp is a leading provider of diagnostic information services and laboratory testing, offering diagnostic testing for conditions ranging

[2] Defendants Laboratory Corporation of America Holdings d/b/a LabCorp; Laboratory Corporation of America d/b/a LabCorp; and America Medical Collection Agency, Inc., are collectively referred to herein as "Defendant Labs." Moreover, Defendants Laboratory Corporation of America Holdings d/b/a LabCorp and Laboratory Corporation of America d/b/a LabCorp are collectively referred to herein as "Defendant LabCorp" or as the "LabCorp Defendants."

from HIV testing, allergy testing, oncology, genetics, and womens' health, among many others.[3]

16. Defendant LabCorp maintains a web portal through which patients can interact with the company and provide a range of Personal Information. The website provides[4]:

> The Online Services can be accessed from the United States and other countries worldwide. Since the laws of each State or country may differ, you agree that the statutes and laws of the State of North Carolina, without regard to any principles of conflicts of law, will apply to all matters relating to your access to or use of the Online Services.

17. Defendant America Medical Collection Agency, Inc. ("AMCA"), is a New York corporation headquartered at 4 Westchester Plaza # 110, Elmsford, NY 10523, and claims to be the Nation's leading recovery agency for patient collections managing over $1 billion in annual receivables for a diverse client base.

## JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction under the Class Action Fairness Act because this is a class action involving more than 100 Class Members, the amount in controversy exceeds $5 million, exclusive of interest and costs, and one or more of the members of the Class reside in a state that is different from the state in which Defendants reside. *See* 28 U.S.C. § 1332(d).

19. This Court has personal jurisdiction over the Defendants as Defendant LabCorp is headquartered and operates in this District, Defendants through their business operations intentionally avail themselves of the markets within this District, and Plaintiffs and Class Members' claims arise out of Defendants' contacts with North Carolina and this District.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391. The LabCorp

[3] *Test Menu*, LabCorp, https://www.labcorp.com/test-menu/search (last visited Aug. 6, 2019).
[4] *Terms and Conditions*, LabCorp, https://www.labcorp.com/hipaa-privacy/terms-and-conditions (last updated May 11, 2017).

Defendants reside in this District and a substantial part of the events and omissions giving rise to the action occurred in this District. Plaintiffs and Class Members received health services from LabCorp Defendants who received and maintained their Personal Information in this District and have caused harm to Plaintiffs and Class Members. All other Defendants are residents of North Carolina.

## STATEMENT OF FACTS

21. LabCorp Defendants are leading providers of medical diagnostic testing services. They perform medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease.

22. LabCorp Defendants' invoices cover laboratory testing fees only and are separate from any bill received by a patient's physician. Patients can be charged by either directly going to a facility operated by Defendants or if their physician has sent their specimen to one of Defendants' facilities.

23. When customers of LabCorp Defendants do not pay their invoices within the requested time period, Defendants will reach out to a collection agency like Defendant AMCA, one of the largest collection agencies in the healthcare sector.

24. LabCorp Defendants provided AMCA with their customers' Personal Information, which they subsequently housed in their own systems, in order to facilitate the collection process.

25. In or around May 14, 2019, AMCA informed LabCorp Defendants of unauthorized activity on AMCA's web payment page.

26. Prior to AMCA informing LabCorp Defendants of the Breach, the security firm Gemini Advisory notified the website databreaches.net that its research had found the payment

card details of 200,000 patients from AMCA for sale on a popular dark web marketplace. The same article reported that AMCA did not respond to Gemini Advisory about the issue, and Gemini instead informed law enforcement.[5] Law enforcement then contacted AMCA.

27. On June 3, 2019, Quest Diagnostics Incorporated ("Quest") publicly announced the following, in relevant part, in a Form 8-K filed with the Securities and Exchange Commission[6]:

> 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
>
> - 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.

28. Also on June 3, 2019, Quest published a press release, stating in part[7]:

> American Medical Collection Agency (AMCA), a billing collections service provider, has informed Quest Diagnostics that an unauthorized user had access to AMCA's system containing personal information AMCA received from various entities,

[5] Jessica Davis, *11.9M Quest Diagnostics Patients Impacted by AMCA Data Breach*, Health IT Security (June 3, 2019), https://healthitsecurity.com/news/11.9m-quest-diagnostics-patients-impacted-by-amca-data-breach.
[6] Quest Form 8-K, SEC (June 3, 2019), https://www.sec.gov/Archives/edgar/data/1022079/000094787119000415/ss138857_8k.htm.
[7] Press Release, Quest Diagnostics Statement on the AMCA Data Security Incident, Quest Diagnostics (June 3, 2019), http://newsroom.questdiagnostics.com/AMCADataSecurityIncident.

> including from Quest. AMCA provides billing collections services to Optum360, which in turn is a Quest contractor. Quest and Optum360 are working with forensic experts to investigate the matter.
>
> AMCA first notified Quest and Optum360 on May 14, 2019 of potential unauthorized activity on AMCA's web payment page. On May 31, 2019, AMCA notified Quest and Optum360 that the data on AMCA's affected system included information regarding approximately 11.9 million Quest patients. AMCA believes this information includes personal information, including certain financial data, Social Security numbers, and medical information, but not laboratory test results.
>
> AMCA has not yet provided Quest or Optum360 detailed or complete information about the AMCA data security incident, including which information of which individuals may have been affected. And Quest has not been able to verify the accuracy of the information received from AMCA.

29. On June 4, 2019, LabCorp Defendants publicly announced the following, in relevant part, in a Form 8-K filed with the Securities and Exchange Commission[8]:

> According to AMCA, this activity occurred between August 1, 2018, and March 30, 2019. AMCA is an external collection agency used by LabCorp and other healthcare companies. LabCorp has referred approximately 7.7 million consumers to AMCA whose data was stored in the affected AMCA system. AMCA's affected system included information provided by LabCorp. That information could include first and last name, date of birth, address, phone, date of service, provider, and balance information. AMCA's affected system also included credit card or bank account information that was provided by the consumer to AMCA (for those who sought to pay their balance). LabCorp 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.
>
> 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.

[8] LabCorp Form 8-K, SEC (June 4, 2019), https://www.sec.gov/Archives/edgar/data/920148/000119312519165091/d757830d8k.htm.

> AMCA has not yet provided LabCorp a list of the affected LabCorp consumers or more specific information about them.

30. In response to this news, a spokesperson for AMCA stated that "upon receiving information from a security compliance firm that works with credit card companies of a possible security compromise, we conducted an internal review, and then took down our web payments page."[9]

31. LabCorp Defendants failed to properly monitor their vendors to ensure that proper and adequate data security safeguards were being implemented by their vendors throughout the breach period so as to properly safeguard Class Members' Personal Information. Had LabCorp Defendants properly monitored their vendor's systems, they would have discovered the intrusion much sooner than eight months after the Breach began.

32. Indeed, it was not until June 4, 2019, over nine months after hackers gained access to their Personal Information, that Plaintiffs received a letter from LabCorp Defendants notifying them of the Breach and the unauthorized access of their Personal Information.

33. Defendants had obligations created by HIPAA, industry standards, common law, and their own representations to Plaintiffs and Class Members to keep their Personal Information confidential and to protect the same from unauthorized access and disclosure.

34. Plaintiffs and Class Members provided their Personal Information to LabCorp Defendants with the reasonable expectation and mutual understanding that LabCorp Defendants and any business partners to which they disclosed the Personal Information, such as Defendants AMCA and Optum360, would comply with their obligations to keep such information confidential and secure from unauthorized access.

[9] Zack Whittaker, *Quest Diagnostics says 11.9 million patients affected by data breach*, TechCrunch (June 3, 2019), https://techcrunch.com/2019/06/03/quest-diagnostics-breach/.

35. The widespread failure to safeguard customers' information was also directly contrary to LabCorp Defendants' representations in their privacy policy that they "contractually require [] third-party vendors and contractors to comply with strict standards regarding security and confidentiality"[10] Defendant LabCorp's Notice of Privacy Practices expressly stated that they are "required by law to maintain the privacy of health information."[11]

36. Defendants' data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the Breach. The increase in data breaches, and the attendant risk of future breaches, was widely known to the public and to anyone in Defendants' industries.

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

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

b. Adequately protecting patients' Personal Information;

c. Properly monitoring their own data security systems for existing intrusions;

d. Ensuring that vendors and contractors employed reasonable data security procedures;

e. Ensuring the confidentiality and integrity of electronic PHI and Personal Information they created, received, maintained, and/or transmitted in violation of 45 C.F.R. § 164.306(a)(1);

f. Implementing technical policies and procedures for electronic information systems that maintain electronic PHI and Personal 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);

g. Implementing policies and procedures to prevent detect, contain, and correct

[10] *Website Privacy Policy*, LabCorp, https://www.labcorp.com/hipaa-privacy/web-privacy-policy (last updated Mar. 25, 2019).
[11] *HIPAA Information*, LabCorp, https://www.labcorp.com/hipaa-privacy/hipaa-information (last updated Apr. 18, 2016).

security breaches in violation of 45 C.F.R. § 164.308(a)(1)(i);

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

i. Protecting against reasonably anticipated threats or hazards to the security or integrity of electronic PHI and Personal Information in violation of 45 C.F.R. § 164.306(a)(2);

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

k. Ensuring compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4); and/or

l. Training all members of their workforces effectively on the policies and procedures regarding PHI and Personal Information as necessary and appropriate for the members of workforces to carry out their functions and to maintain security of PHI and Personal Information in violation of 45 C.F.R. § 164.530(b).

38. Plaintiffs and Class Members have been damaged by the compromise and unauthorized disclosure of their Personal Information in the Breach.

39. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billing in their names, tax-return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

40. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Personal Information as hackers could use that information to more effectively target such schemes to Plaintiffs and Class Members.

41. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Breach.

42. Plaintiffs and Class Members suffered a "loss of value" of their Personal Information when it was acquired by cyber criminals in the Breach.

43. Plaintiffs and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiffs and Class Members paid to Defendants was intended to be used by Defendants to fund adequate data security and to monitor their vendors' compliance with data security obligations, including AMCA and Optum360. Defendants did not properly monitor AMCA, Optum360, and other vendors' compliance with data security obligations. Plaintiffs and Class Members did not get what they paid for.

44. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time and effort to monitor their financial, personal and medical accounts for misuse.

45. On an all too frequent basis, data thieves use identifying data such as Social Security numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name. This type of identity theft is particularly harmful because it often takes time for the victim to become aware of the theft, and the theft can adversely impact the victim for years.

46. There may be a substantial time lag—measured in years—between when Personal Information is stolen and when it is used. Thus, Plaintiffs and Class Members must vigilantly monitor their financial, personal and medical accounts for many years to come.

47. With access to the type of information that was accessed in the Breach, criminals can use the information gained to gather additional information about Plaintiffs and Class Members; open accounts in the victim's name; receive medical services in the victim's name; obtain a driver's license or official identification card in the victim's name but with the

criminal's photo; use the victim's name and Social Security number to obtain government benefits; file a fraudulent tax return using the victim's information; and give the victim's Personal Information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.

48. Social Security numbers, for example, are among the worst kind of Personal Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

49. Stolen Social Security numbers make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. And fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not possible. Plaintiffs and Class Members now live with this reality.

50. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often sell it on the "black-market" or "dark web" indefinitely. Cyber criminals routinely post stolen Social Security numbers, financial information, medical information, and other private information on anonymous websites, making the information widely available to a criminal underworld. There is an active and robust market for this information.

51. Medical information is especially valuable to identity thieves. Because of its value, the medical industry has experienced disproportionally higher numbers of data thefts than

other industries. Defendants knew or should have known this and strengthened their data systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

## CLASS ACTION ALLEGATIONS

52. Plaintiffs bring this complaint on behalf of themselves and the following Class Members ("Nationwide Class"):

> All persons who provided Personal Information to Defendants and whose Personal Information was compromised as a result of the Breach.

53. Plaintiff Driskell ("Alabama Plaintiff") also seeks certification of the following state Subclass ("Alabama Subclass"):

> All persons residing in Alabama who provided Personal Information to Defendants and whose Personal Information was compromised as a result of the Breach.

54. Plaintiffs Aponte, Grushka, and Stone ("Florida Plaintiffs") also seek certification of the following state Subclass ("Florida Subclass"):

> All persons residing in Florida who provided Personal Information to Defendants and whose Personal Information was compromised as a result of the Breach.

55. Plaintiffs Martin and Stanford ("Georgia Plaintiffs") also seek certification of the following state Subclass ("Georgia Subclass"):

> All persons residing in Georgia who provided Personal Information to Defendants and whose Personal Information was compromised as a result of the Breach.

56. Plaintiff Storey ("Kentucky Plaintiff") also seeks certification of the following state Subclass ("Kentucky Subclass"):

> All persons residing in Kentucky who provided Personal Information to Defendants and whose Personal Information was compromised as a result of the Breach.

57. Plaintiff Parrott ("Louisiana Plaintiff") also seeks certification of the following state Subclass ("Louisiana Subclass"):

> All persons residing in Louisiana who provided Personal Information to Defendants and whose Personal Information was compromised as a result of the Breach.

58. Plaintiff Schwall ("North Carolina Plaintiff") also seeks certification of the following state Subclass ("North Carolina Subclass"):

> All persons residing in North Carolina who provided Personal Information to Defendants and whose Personal Information was compromised as a result of the Breach.

59. Plaintiff Steed ("South Carolina Plaintiffs") also seeks certification of the following state Subclass ("South Carolina Subclass"):

> All persons residing in South Carolina who provided Personal Information to Defendants and whose Personal Information was compromised as a result of the Breach.

60. Plaintiffs reserve the right to propose other Subclasses prior to trial.

61. The Class and Subclasses specifically exclude: (a) any persons or other entities currently related to or affiliated with Defendants; (b) any Judge presiding over this action and members of his or her family; and (c) all persons who properly execute and file a timely request for exclusion.

62. Class-wide adjudication of Plaintiffs' claims is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

63. *Numerosity*: The members of the putative Class, estimated at 19.6 million, are so numerous that joinder of individual claims is impracticable. Members of the Class can be readily identified through Defendants' records.

64. *Commonality*: There are significant questions of fact and law common to the

members of the Class. These issues include but are not limited to:

a. Whether Defendants failed to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

b. Whether Defendants failed to maintain adequate data security policies, procedures, and practices to secure Plaintiffs and Class Members' Personal Information;

c. Whether the security provided by Defendants was satisfactory to protect customer information as compared to industry standards;

d. Whether Defendants misrepresented or failed to provide adequate information to customers regarding the type of security practices used;

e. Whether Defendants' conduct was intentional, willful or negligent;

f. Whether Defendants violated any and all statutes and/or common law listed herein;

g. Whether the Plaintiffs and Class Members suffered damages as a result of Defendants' conduct or omissions; and

h. Whether Plaintiffs and Class Members are entitled to injunctive, declarative and monetary relief as a result of Defendants' conduct.

65. *Typicality*: Plaintiffs' claims are typical of the claims of the proposed Class. Plaintiffs and all members of the proposed Class have been adversely affected and damaged in that Defendants failed to adequately protect their Personal Information to the detriment of Plaintiffs and the proposed Class.

66. *Adequacy of Representation*: Plaintiffs, as the proposed Class Representatives, will fairly and adequately represent the proposed Class because they have Class Members' best interest in mind, because their individual claims are co-extensive with those of the Class, and because they are represented by qualified counsel experienced in class action litigation of this nature.

67. *Superiority*: A class action in this instance is superior to other available methods for the fair and efficient adjudication of these claims because individual joinder of the claims of

all members of the proposed Class is impracticable. Many members of the Class are without the financial resources necessary to pursue this matter. Even if some members of the Class could afford to litigate their claims separately, such a result would be unduly burdensome to the courts in which the individualized cases would proceed. Individual litigation increases the time and expense of resolving a common dispute concerning Defendants' actions toward an entire group of individuals. Class action procedures allow for far fewer management difficulties in matters of this type and provide the unique benefits of unitary adjudication, economies of scale and comprehensive supervision over the entire controversy by a single judge in a single court.

68. The proposed Class may be certified pursuant to Rule 23(b)(2) of the Federal Rules of Civil Procedure because Defendants have acted on grounds generally applicable to the proposed Class, thereby making final injunctive relief and corresponding declaratory relief appropriate with respect to the claims raised by the Class.

69. The proposed Class may also be certified pursuant to Rule 23(b)(3) of the Federal Rules of Civil Procedure because questions of law and fact common to Class Members will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

## COUNT 1

## *BREACH OF IMPLIED CONTRACT*

70. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

71. When Plaintiffs and Class Members provided their Personal Information to Defendants in exchange for Defendants' services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

72. Defendants solicited and invited Plaintiffs and Class Members to provide their

Personal Information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their Personal Information to Defendants.

73. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

74. Plaintiffs and Class Members were aware of, or reasonably anticipated that, LabCorp Defendants would forward certain Personal Information to vendors, such as AMCA and Optum360.

75. Plaintiffs and Class Members who paid money to Defendants (either directly or indirectly) reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

76. Plaintiffs and Class Members would not have entrusted their Personal Information to LabCorp Defendants in the absence of the implied contracts between them and LabCorp Defendants to keep the information reasonably secure. Plaintiffs and Class Members would not have entrusted their Personal Information to LabCorp Defendants in the absence of LabCorp Defendants' implied promise to monitor its vendors, such as AMCA and Optum360, to ensure that they adopted reasonable data security measures.

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

78. Defendants breached their implied contract with Class Members by failing to safeguard and protect their Personal Information. Defendants also breached their implied contract with Class Members by failing to properly monitor the data security practices of their vendors.

79. As a direct and proximate result of Defendants' breaches of the implied contracts, Class Members sustained damages as alleged herein.

80. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Breach.

81. Plaintiffs and Class Members are also entitled to injunctive relief.

## COUNT 2

### *NEGLIGENCE*

82. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

83. Defendants required Plaintiffs and Class Members to submit non-public Personal Information in order to obtain medical services, which they forwarded to AMCA and Optum360 for billing purposes.

84. By collecting and storing this data, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard Class Members' Personal Information, to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

85. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Personal Information.

86. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and their client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law.

Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

87. Defendants' duty to use reasonable security measures under HIPAA required 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). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

89. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect Personal Information.

90. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Personal Information, and by failing to provide timely notice of the Breach. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Personal Information;

b. Failing to adequately monitor the security of AMCA, Optum360, and other vendors' networks and systems;

c. Failure by Defendants to periodically ensure that their vendors, including AMCA and Optum360, had procedures in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Personal Information;

e. Failing to detect in a timely manner that Class Members' Personal Information had been compromised; and

f. Failing to timely notify Class Members about the Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

91. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Personal Information would result in injury to Class Members. Further, the Breach was reasonably foreseeable given the known high frequency of data breaches in the medical industry.

92. It was therefore foreseeable that the failure to adequately safeguard Class Members' Personal Information would result in one or more types of injuries to Class Members.

93. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Breach.

94. Plaintiffs and Class Members are also entitled to injunctive relief.

**COUNT 3**

***NEGLIGENCE PER SE***

95. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

96. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Personal Information.

97. Pursuant to HIPAA (42 U.S.C. § 1302d *et seq*.), Defendants had a duty to implement reasonable safeguards to protect Plaintiffs and Class Members' Personal Information.

98. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendants had a duty to protect the security and confidentiality of Plaintiffs and Class Members' Personal Information.

99. Defendants breached their duties to Plaintiffs and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45); HIPAA (42 U.S.C. § 1302d, *et. seq.*); and the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) by failing to provide fair, reasonable, and/or adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Personal Information.

100. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

101. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

102. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants' breaches of their duties. Defendants knew or should have known that they were failing to satisfy their duties, and that Defendants' breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

103. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

## COUNT 4

## *BREACH OF DUTY OF GOOD FAITH AND FAIR DEALING*

104. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

105. In light of the special relationship between Defendants and Plaintiffs and Class Members, whereby Defendants became guardians of Plaintiffs and Class Members' Personal Information, Defendants became fiduciaries created by their undertaking and guardianship of the Personal Information, to act primarily for the benefit of their patients, including Plaintiffs and

Class Members, (1) for the safeguarding of Plaintiffs and Class Members' Personal Information; (2) to timely notify Plaintiffs and Class Members of a data breach and disclosure; and (3) maintain complete and accurate records of what and where Defendants' patient information was and is stored.

106. Defendants have a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their patients' relationship, in particular, to keep secure the Personal Information of the patients.

107. Defendants breached their fiduciary duties to Plaintiffs and Class Members by failing to diligently investigate the Breach to determine the number of Class Members affected in a reasonable and practicable period of time.

108. Defendants breached their fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs and Class Members' Personal Information.

109. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Breach.

110. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendants created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

111. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by failing to 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).

112. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

113. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

114. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2).

115. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

116. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. § 164.306(a)(94).

117. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502 *et seq*.

118. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by failing to effectively train all members of Defendants' workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the

members of the workforce to carry out their functions and to maintain the security of protected health information in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

119. Defendants breached their fiduciary duties owed to Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c).

120. Defendants breached their fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs and Class Members' Personal Information.

121. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to, the following: (i) actual identity theft; (ii) the loss of the opportunity to know how their Personal Information is used; (iii) the compromise, publication, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Personal Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Personal Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Personal Information in their continued possession; (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Breach for the remainder of the lives of Plaintiffs and Class Members; and (viii) the

diminished value of Defendants' services they received.

122. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

**COUNT 5**

***INVASION OF PRIVACY***

123. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

124. Defendants invaded Plaintiffs and Class Members' right to privacy by allowing the unauthorized access to Plaintiffs and Class Members' Personal Information and by negligently maintaining the confidentiality of Plaintiffs and Class Members' Personal Information, as set forth above.

125. The intrusion was offensive and objectionable to Plaintiffs, Class Members, and to a reasonable person of ordinary sensibilities in that Plaintiffs and Class Members' Personal Information was disclosed without prior written authorization of Plaintiffs and Class Members.

126. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiffs and Class Members provided and disclosed their Personal Information to Defendants privately with an intention that the Personal Information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and Class Members reasonably believed that such information would be kept private and would not be disclosed without their written authorization.

127. As a proximate result of Defendants' acts as alleged herein, Plaintiffs' and Class Members' Personal Information was viewed, printed, distributed, and used by persons without prior written authorization and Plaintiffs and Class Members suffered damages as a result.

128. Defendants' unauthorized disclosure of Plaintiffs and Class Members' Personal

Information occurred as a result of Defendants' willful and conscious disregard of Plaintiffs and Class Members' right to privacy.

129. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause Plaintiffs and Class Members great and irreparable injury in that the Personal Information maintained by Defendants can be viewed, printed, distributed, and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy into Plaintiffs and Class Members' Personal Information.

**COUNT 6**

***DECLARATORY RELIEF***

130. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

131. Pursuant to the Declaratory Judgment Act, 28 U.S.C. § 2201 and Rule 57 of the Federal Rules of Civil Procedure, Plaintiffs and Class Members respectfully request for the Court to enter a judgment declaring, *inter alia,* (i) Defendants owed (and continue to owe) a legal duty to safeguard and protect Plaintiffs and Class Members' Personal Information and a legal duty to timely notify them about any security breach; (ii) Defendants breached (and continue to breach) such legal duties by failing to safeguard and protect Plaintiffs and Class Members' Personal Information; and (iii) Defendants' breach of their legal duties directly and proximately caused the Breach, and the resulting damages, injury, and harm suffered by Plaintiffs and Class Members.

**COUNT 7**

***INJUNCTIVE RELIEF***

132. Plaintiffs reallege, as if fully set forth, the allegations of the preceding paragraphs.

133. Defendants' above-described wrongful actions, inactions, omissions, want of

ordinary care, nondisclosures, and the resulting security breach have caused (and will continue to cause) Plaintiffs and Class Members to suffer irreparable harm in the form of economic damages and other injury and actual harm including, but not limited to, (i) actual identity theft and identity fraud; (ii) invasion of privacy; (iii) loss of the intrinsic value of their privacy; (iv) breach of the confidentiality of their consumer reports and consumer credit information; (v) deprivation of the value of their consumer credit information, for which there is a well- established national and international market; (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages; and (vii) the imminent, immediate, and continuing increased risk of ongoing identity theft and identity fraud. Such irreparable harm will not cease unless and until enjoined by this Court.

134. Plaintiffs and Class Members, therefore, are entitled to injunctive relief and other appropriate affirmative relief including, but not limited to, an order compelling Defendants to, *inter alia*, (i) notify each person whose Personal Information was exposed in the Breach; (ii) provide credit monitoring to each such person for at least six years; (iii) establish a fund (in an amount to be determined) to which such persons may apply for reimbursement of the time and out-of-pocket expenses they incurred to remediate identity theft and/or identity fraud (*i.e.*, data breach insurance); and (iv) discontinue the above-described wrongful actions, inactions, omissions, want of ordinary care, and nondisclosures.

135. Plaintiffs and Class Members also are entitled to injunctive relief compelling Defendants to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' computer systems on a periodic

basis; (ii) engaging third-party security auditors and internal personnel to run automated security monitoring; (iii) auditing, testing, and training their security personnel regarding any new or modified procedures; (iv) conducting regular database scanning and security checks; (v) regularly evaluating web applications for vulnerabilities to prevent web application threats; and (vi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain data security lapses.

136. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury in the event Defendants commit another security lapse, the risk of which is real, immediate, and substantial.

137. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if Defendants suffer another massive security lapse, Plaintiffs and Class Members will likely again incur millions of dollars in damages. On the other hand, and setting aside the fact that Defendants have a pre-existing legal obligation to employ adequate customer data security measures, the cost for Defendants to comply with the above-described injunction that they are already required to implement is relatively minimal.

138. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another security breach, thereby eliminating the damages, injury, and harm that would be suffered by Plaintiffs, Class Members, and the millions of consumers whose Personal Information would be compromised.

## COUNT 8

### *ALABAMA DECEPTIVE TRADE PRACTICES ACT*
### **Ala. Code §§ 8-19-1 *et seq.***

139. Alabama Plaintiffs identified above ("Plaintiffs," for purposes of this Count),

individually and on behalf of the Alabama Subclass, repeats and alleges all previous Paragraphs as if fully alleged herein.

140. Defendants are "persons" as defined by Ala. Code § 8-19-3(5).

141. Plaintiffs and Alabama Subclass Members are "consumers" as defined by Ala. Code § 8-19-3(2).

142. Defendants advertised, offered, or sold goods or services in Alabama, and engaged in trade or commerce directly or indirectly affecting the people of Alabama.

143. Defendants engaged in deceptive acts and practices in the conduct of trade or commerce, in violation of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, including:

144. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;

145. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and

146. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce, including acts and practices that would violate Section 5(a)(1) of the FTC Act, as interpreted by the FTC and federal courts.

147. Defendants' deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Alabama Subclass Members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Alabama Subclass Members' Personal Information,

including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Alabama Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alabama Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Alabama Subclass Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Alabama Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

148. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

149. Defendants intended to mislead Plaintiffs and Alabama Subclass Members and induce them to rely on its misrepresentations and omissions.

150. Had Defendants disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

151. Defendants accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public. Accordingly, because Defendants held itself out as being trustworthy and secure, Plaintiffs and the Alabama Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth

of which they could not have discovered.

152. Defendants acted intentionally, knowingly, and maliciously to violate the Alabama Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Alabama Subclass Members' rights. past data breaches put it on notice that its security and privacy protections were inadequate.

153. As a direct and proximate result of Defendants' deceptive acts and practices, Plaintiffs and Alabama Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

154. Defendants' deceptive acts and practices caused substantial injury to Plaintiffs and Alabama Subclass Members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

155. Plaintiffs and the Alabama Subclass seek all monetary and nonmonetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of $100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

## COUNT 9

### *FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT*
### **Fla. Stat. §§ 501.201 *et seq.***

156. Florida Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the Florida Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

157. Plaintiffs and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

158. Defendants advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

159. Defendants engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including, but not limited to, the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Florida Subclass Members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Florida Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, Fla. Stat. § 501.171(2), which was a direct and proximate cause of the Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs and Florida Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Florida Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, Fla. Stat. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs and Florida Subclass Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Florida Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Florida's data security statute, Fla. Stat. § 501.171(2).

160. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

161. Had Defendants disclosed to Plaintiffs and Florida Subclass Members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants held themselves out as secure and were entrusted with the Personal Information regarding millions of consumers, including Plaintiffs and Florida Subclass Members.

162. Defendants accepted the responsibility of being "stewards of data" while keeping the inadequate state of their security controls secret from the public.

163. Plaintiffs and Florida Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

164. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and practices, Plaintiffs and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased and imminent risk of fraud and identity theft; and loss of value of their Personal Information.

165. Plaintiffs and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs under Fla. Stat. § 501.2105(1); and any

other relief that is just and proper.

## COUNT 10

### *GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT*
### GA. CODE ANN. §§ 10-1-370 *et seq.*

166. Georgia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

167. Defendants, Plaintiff, and Georgia Subclass Members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

168. Defendants engaged in deceptive trade practices in the conduct of its business, in violation of Ga. Code Ann. § 10-1-372(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

169. Defendants' deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Georgia Subclass Members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Georgia Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Georgia Subclass Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

170. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

171. Defendants intended to mislead Plaintiff and Georgia Subclass Members and induce them to rely on its misrepresentations and omissions.

172. In the course of its business, Defendants engaged in activities with a tendency or capacity to deceive.

173. Defendants acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Georgia Subclass Members' rights. Past data breaches put Defendants on notice that its security and privacy protections were inadequate.

174. Had Defendants disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants held itself out as Secure and was trusted with sensitive

and valuable Personal Information regarding millions of consumers, including Plaintiff and the Georgia Subclass.

175. Defendants accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

176. Plaintiff and the Georgia Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

177. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff and Georgia Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

178. Plaintiff and Georgia Subclass Members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under Ga. Code Ann. § 10-1-373.

## COUNT 11

### *KENTUCKY COMPUTER SECURITY BREACH NOTIFICATION ACT*
### **Ky. Rev. Stat. Ann. §§ 365.732 *et seq.***

179. Kentucky Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

180. Defendants are required to accurately notify Plaintiffs and Kentucky Subclass Members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs' and Kentucky Subclass Members'

Personal Information, in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

181. Each Defendant is a business that holds computerized data that includes Personal Information as defined by Ky. Rev. Stat. Ann. § 365.732(2).

182. Plaintiffs' and Kentucky Subclass Members' PII includes Personal Information as covered under Ky. Rev. Stat. Ann. § 365.732(2).

183. Because Defendants was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs' and Kentucky Subclass Members' Personal Information, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

184. By failing to disclose the Breach in a timely and accurate manner, Defendants violated Ky. Rev. Stat. Ann. § 365.732(2).

185. As a direct and proximate result of Defendants' violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiffs and Kentucky Subclass Members suffered damages, as described above.

186. Plaintiff and Kentucky Subclass Members seek relief under Ky. Rev. Stat. Ann. § 446.070, including actual damages.

## COUNT 12

### *KENTUCKY CONSUMER PROTECTION ACT*
### **Ky. Rev. Stat. §§ 367.110 *et seq.***

187. Kentucky Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

188. Defendants are "persons" as defined by Ky. Rev. Stat. § 367.110(1).

189. Defendants advertised, offered, or sold goods or services in Kentucky and

engaged in trade or commerce directly or indirectly affecting the people of Kentucky, as defined by Ky. Rev. Stat. 367.110(2).

190. Defendants engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. § 367.170, including:

191. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kentucky Subclass Members' Personal Information, which was a direct and proximate cause of the Breach;

a. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and Kentucky Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

d. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Kentucky Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Kentucky Subclass Members' Personal Information; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

192. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

193. Defendants intended to mislead Plaintiffs and Kentucky Subclass Members and induce them to rely on its misrepresentations and omissions.

194. Plaintiffs and Kentucky Subclass Members' purchased goods or services for personal, family, or household purposes and suffered ascertainable losses of money or property as a result of Defendants' unlawful acts and practices.

195. The above unlawful acts and practices by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Kentucky Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

196. Defendants acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiffs and Kentucky Subclass Members' rights. Past breaches put it on notice that its security and privacy protections were inadequate.

197. As a direct and proximate result of Defendants' unlawful acts and practices, Plaintiffs and Kentucky Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

198. Plaintiffs and Kentucky Subclass Members seek all monetary and nonmonetary relief allowed by law, including damages, punitive damages, restitution or other equitable relief, injunctive relief, and reasonable attorneys' fees and costs.

## COUNT 13

***LOUISIANA DATABASE SECURITY BREACH NOTIFICATION LAW***
**La. Stat. Ann. §§ 51:3074(A) *et seq.***

199. Louisiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

200. Each Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by La. Stat. Ann. § 51:3074(C).

201. Plaintiff's and Louisiana Subclass Members' PII includes Personal Information as covered under La. Stat. Ann. § 51:3074(C).

202. Defendants are required to accurately notify Plaintiff and Louisiana Subclass Members if they become aware of a breach of their data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass Members' Personal Information, in the most expedient time possible and without unreasonable delay under La. Stat. Ann. § 51:3074(C).

203. Because Defendants was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass Members' Personal Information, Defendants had an obligation to disclose the Defendants data breach in a timely and accurate fashion as mandated by La. Stat. Ann. § 51:3074(C).

204. By failing to disclose the Defendants data breach in a timely and accurate manner, Defendants violated La. Stat. Ann. § 51:3074(C).

205. As a direct and proximate result of Defendants' violations of La. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Subclass Members suffered damages, as described above.

206. Plaintiff and Louisiana Subclass Members seek relief under La. Stat. Ann. § 51:3075, including actual damages.

## COUNT 14

### *LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW*
### La. Stat. Ann. §§ 51:1401 *et seq.*

207. Louisiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and alleges all previous Paragraphs, as if fully alleged herein.

208. Defendants, Plaintiff, and the Louisiana Subclass Members are "persons" within the meaning of the La. Stat. Ann. § 51:1402(8).

209. Plaintiff and Louisiana Subclass Members are "consumers" within the meaning of La. Stat. Ann. § 51:1402(1).

210. Defendants engaged in "trade" or "commerce" within the meaning of La. Stat. Ann. § 51:1402(10).

211. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes unlawful "unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

212. Defendants participated in unfair and deceptive acts and practices that violated the Louisiana CPL, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Louisiana Subclass Members' Personal Information, which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Louisiana Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Louisiana Subclass Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

213. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

214. Defendants intended to mislead Plaintiff and Louisiana Subclass Members and induce them to rely on its misrepresentations and omissions.

215. Defendants' unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

216. Defendants acted intentionally, knowingly, and maliciously to violate Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Louisiana Subclass Members' rights. Past data breaches put Defendants on notice that its

security and privacy protections were inadequate.

217. Had Defendants disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants held itself out as secure and was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Louisiana Subclass.

218. Defendants accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

219. Plaintiff and the Louisiana Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

220. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff and Louisiana Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

221. Plaintiff and Louisiana Subclass Members seek all monetary and nonmonetary relief allowed by law, including actual damages; treble damages for Defendants' knowing violations of the Louisiana CPL; declaratory relief; attorneys' fees; and any other relief that is just and proper.

## COUNT 15

### *NORTH CAROLINA UNFAIR TRADE PRACTICES ACT*
### N.C. Gen. Stat. §§ 75-1.1 *et seq.*

222. North Carolina Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

223. Defendants are subject to the laws and regulations of the State of North Carolina, including but not limited to the North Carolina Unfair & Deceptive Trade Practices Act, N.C. Gen. Stat. § 75-1.1 ("North Carolina UDTPA"). The North Carolina UDTPA "declare[s] unlawful" all "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." *Id.* § 75-1.1(a).

224. For purposes of North Carolina UDTPA, the term "'commerce' includes all business activities, however denominated, but does not include professional services rendered by a member of a learned profession." *Id.* § 75-1.1(b).

225. Defendants violated the North Carolina UDTPA by engaging in unlawful, unfair, or deceptive business acts and practices in or affecting commerce, as well as unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" prohibited by the North Carolina UDTPA.

226. Defendants engaged in unlawful acts and practices with respect to their services by establishing inadequate security practices and procedures described herein; by soliciting and collecting Plaintiff's and North Carolina Subclass Members' Personal Information with knowledge that such information would not be adequately protected; and by gathering Plaintiff's and North Carolina Subclass Members' Personal Information in an unsecure electronic environment in violation of North Carolina's data breach statute, the Identity Theft Protection

Act, N.C. Gen. Stat. § 75-60 *et seq.*, which requires Defendants to undertake reasonable methods of safeguarding the Personal Information of Plaintiff and North Carolina Subclass Members.

227. In addition, Defendants engaged in unlawful acts and practices when they failed to discover and then disclose the data security breach to Plaintiff and North Carolina Subclass Members in a timely and accurate manner, contrary to the duties imposed by N.C. Gen. Stat. § 75-65.

228. To date, Defendants still have not provided sufficient information regarding the Breach to Plaintiff and North Carolina Subclass Members.

229. As a direct and proximate result of Defendants' unlawful acts and practices, Plaintiff and North Carolina Subclass Members were injured and lost money or property, including but not limited to the loss of their legally protected interests in the confidentiality and privacy of their Personal Information.

230. Defendants knew or should have known that their data security practices were inadequate to safeguard Plaintiff's and North Carolina Subclass Members' Personal Information, that the risk of a data security breach was significant, and that their system was, in fact, breached.

231. Defendants' actions in engaging in the above-described unlawful practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and North Carolina Subclass Members.

232. Plaintiff and North Carolina Subclass Members seek relief under the North Carolina UDTPA including, but not limited to, the following: restitution to Plaintiff and North Carolina Subclass Members of money and property that Defendants acquired by means of unlawful and unfair business practices; disgorgement of all profits accruing to Defendants

because of their unlawful and unfair business practices; treble damages (pursuant to N.C. Gen. Stat. § 75-16); declaratory relief; attorneys' fees and costs (pursuant to N.C. Gen. Stat. § 75-16.1); and injunctive or other equitable relief.

## COUNT 16

### *NORTH CAROLINA IDENTITY THEFT PROTECTION ACT*
### N.C. Gen. Stat. §§ 75-60 *et seq*.

233. North Carolina Plaintiff identified above ("Plaintiff" for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

234. Defendants are businesses that own or license computerized data that includes Personal Information as defined by N.C. Gen. Stat. § 75-61(1).

235. Plaintiff and North Carolina Subclass Members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

236. Defendants are required to accurately notify Plaintiff and North Carolina Subclass Members if they discover a security breach, or receives notice of a security breach (*i.e.*, where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons) without unreasonable delay under N.C. Gen. Stat. § 75-65.

237. Plaintiff and North Carolina Subclass Members' Personal Information includes Personal Information as covered under N.C. Gen. Stat. § 75-61(10).

238. Because Defendants discovered a security breach and had notice of a security breach, namely the Breach, Defendants had an obligation to disclose the Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

239. By failing to disclose the Breach in a timely and accurate manner, Defendants violated N.C. Gen. Stat. § 75-65.

240. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. § 75-1.1.

241. As a direct and proximate result of Defendants' violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina Subclass Members suffered damages, as described above.

242. Plaintiff and North Carolina Subclass Members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorneys' fees.

## COUNT 17

### *SOUTH CAROLINA DATA BREACH SECURITY ACT*
### S.C. Code Ann. §§ 39-1-90 *et seq.*

243. South Carolina Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

244. Each Defendant is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

245. Plaintiffs' and South Carolina Subclass Members' PII includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

246. Defendants are required to accurately notify Plaintiffs and South Carolina Subclass Members following discovery or notification of a breach of their data security system if Personal Information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

247. Because Defendants discovered a breach of its data security system in which Personal Information that was not rendered unusable through encryption, redaction, or other

methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, Defendants had an obligation to disclose the Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

248. By failing to disclose the Breach in a timely and accurate manner, Defendants violated S.C. Code Ann. § 39-1-90(A).

249. As a direct and proximate result of Defendants' violations of S.C. Code Ann. § 39-1-90(A), Plaintiffs and South Carolina Subclass Members suffered damages, as described above.

250. Plaintiffs and South Carolina Subclass Members seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages and injunctive relief.

## COUNT 18

### *SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT*
### S.C. Code Ann. §§ 39-5-10 *et seq.*

251. South Carolina Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeat and allege all previous Paragraphs, as if fully alleged herein.

252. Each Defendant is a "person," as defined by S.C. Code Ann. § 39-5-10(a).

253. South Carolina's Unfair Trade Practices Act (SC UTPA) prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code Ann. § 39-5-20.

254. Defendants advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

255. Defendants engaged in unfair and deceptive acts and practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and South Carolina Subclass Members' Personal Information,

which was a direct and proximate cause of the Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and South Carolina Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and South Carolina Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and South Carolina Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and South Carolina Subclass Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and South Carolina Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

256. Defendants' acts and practices had, and continue to have, the tendency or capacity to deceive.

257. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

258. Defendants intended to mislead Plaintiffs and South Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

259. Had Defendants disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue

in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants held itself out as secure and was trusted with sensitive and valuable Personal Information regarding millions of consumers, including Plaintiffs and the South Carolina Subclass.

260. Defendants accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

261. Plaintiffs and the South Carolina Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

262. Defendants had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensiveness of the Personal Information in its possession, and the generally accepted professional standards.

263. Such a duty is also implied by law due to the nature of the relationship between consumers—including Plaintiffs and the South Carolina Subclass—and Defendants, because consumers are unable to fully protect their interests with regard to the Personal Information in Defendants' possession, and place trust and confidence in Defendants.

264. Defendants' duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the South Carolina Subclass that contradicted these representations.

265. Defendants' business acts and practices offend an established public policy, or are immoral, unethical, or oppressive. Defendants' acts and practices offend established public

policies that seek to protect consumers' Personal Information and ensure that entities entrusted with Personal Information use appropriate security measures. These public policies are reflected in laws such as the FTC Act, 15 U.S.C. § 45 and the South Carolina Data Breach Security Act, S.C. Code § 39-1-90 *et seq.*

266. Defendants' failure to implement and maintain reasonable security measures was immoral, unethical, or oppressive in light of Defendants' long history of inadequate data security and previous data breaches; the sensitivity and extensiveness of Personal Information in its possession.

267. Defendants' unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition; Defendants engages in such acts or practices as a general rule; and such acts or practices impact the public at large.

268. Defendants' unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions occurred in the past, including numerous past data breaches, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, Defendants' policies and procedures, such as its security practices, create the potential for recurrence of the complained-of business acts and practices.

269. Defendants' violations present a continuing risk to Plaintiffs and South Carolina Subclass Members as well as to the general public.

270. Defendants intended to mislead Plaintiffs and South Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

271. Defendants acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiffs and South Carolina Subclass Members' rights. Past data breaches put it on notice that its security and privacy

protections were inadequate. In light of this conduct, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct and would deter Defendants and others from committing similar conduct in the future.

272. As a direct and proximate result of Defendants' unfair and deceptive acts or practices, Plaintiffs and South Carolina Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

273. Plaintiffs and South Carolina Subclass Members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses; treble damages; punitive damages; injunctive relief; and reasonable attorneys' fees.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of Class Members, respectfully request that the Court enter a judgment against Defendants including the following:

a. Determining that this matter may proceed as a class action and certifying the classes asserted herein;

b. Designating Plaintiffs as Class Representatives and Plaintiffs' counsel as Class Counsel;

c. Awarding Plaintiffs and the Class compensatory, consequential, and punitive damages;

d. Granting declaratory and injunctive relief as set forth above;

e. Awarding attorneys' fees, litigation expenses and costs of suit incurred through the trial and any appeals of this case;

f. Awarding pre- and post-judgment interest, as provided by law or equity; and

g. Such other and further relief the Court deems just and proper.

## JURY DEMAND

Plaintiffs, individually and on behalf of Class Members, respectfully demand a trial by jury on all claims and causes of action so triable.

Dated: August 12, 2019

Respectfully submitted,

*/s/ Daniel K. Bryson*

Daniel K. Bryson (NC Bar No. 15781)
**WHITFIELD BRYSON & MASON LLP**
900 W. Morgan Street
Raleigh, NC 27603
Tel: (919) 600-5002
Fax: (919) 600-5035
dan@wbmllp.com

Gary E. Mason (*pro hac vice* forthcoming)
**WHITFIELD BRYSON & MASON LLP**
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Tel: (202) 640-1168
Fax: (202) 429-2294
gmason@wbmllp.com

Charles S. Schaffer (*pro hac vice* forthcoming)
Nicholas J. Elia (*pro hac vice* forthcoming)
**LEVIN SEDRAN & BERMAN LLP**
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: (215) 592-1500
cschaffer@lfsblaw.com
nelia@lfsblaw.com