Exhibit B

James E. Cecchi
CARELLA BYRNE CECCHI
OLSTEIN BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
(973) 994-1700
Interim Lead Counsel for Plaintiffs
(Additional Counsel on the Signature Page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE: AMERICAN MEDICAL COLLECTION AGENCY, INC. CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: All Actions Against Laboratory Corporation of America Holdings	Civil Action No. 19-md-2904 (MCA)(MAH) **CONSOLIDATED CLASS ACTION COMPLAINT: LABCORP**

TABLE OF CONTENTS

TABLE OF CONTENTS
(Cont'd)

TABLE OF CONTENTS
(Cont'd)

Plaintiffs, individually and on behalf of a class of all those similarly situated (the "Class" or "Class Members"), upon personal knowledge of the facts pertaining to Plaintiffs and on information and belief as to all other matters, and upon the investigation conducted by Plaintiffs' counsel, complain against Laboratory Corporation of America Holdings ("LabCorp" or "Defendant"), and allege as follows:

PRELIMINARY STATEMENT

1. On June 4, 2019, LabCorp revealed in a securities filing that an unauthorized user or users accessed the system run by LabCorp's billing collections vendor, Retrieval-Masters Creditor's Bureau, Inc., d/b/a American Medical Collection Agency ("AMCA"), between August 2018 and March 2019 (the "Data Breach"). After accessing AMCA's systems, the hacker exfiltrated the sensitive personal, financial, and health testing information of millions of LabCorp patients and sold the information for profit on underground websites known as the "dark web." [1]

2. Plaintiffs bring this class action because Defendant failed in its basic, legally-bound, and expressly-promised obligation to secure and safeguard LabCorp patients' protected health information ("PHI") and personally identifiable information ("PII")—such as Plaintiffs' and Class Members' names, mailing addresses, phone numbers, dates of birth, Social Security numbers, information related to Plaintiffs' and Class Members' medical providers and services (such as dates of service and referring doctor) and other private information, such as credit and

[1] The dark web refers to encrypted content online that cannot be found using conventional search engines and can only be accessed through specific browsers and software. MacKenzie Sigalos, *The dark web and how to access it* (Apr. 14, 2018), https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html (last accessed June 17, 2019).

debit card numbers, bank account information, insurance, and insurance subscriber identification numbers (all collectively referred to as "Personal Information").

3. As of today, more than 10.2 million LabCorp patients have had their Personal Information compromised as a result of the Data Breach. As a result of Defendant's failure to protect the Personal Information it was entrusted—and legally obligated—to safeguard, Plaintiffs and Class Members suffered a loss of value of their Personal Information and have been exposed to and/or are at imminent and significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. In fact, some Class Members' identities have already likely been stolen.

4. Defendant could have prevented this theft had it limited the customer information it shared with its business associates and employed reasonable measures to ensure its business associates implemented and maintained adequate data security measures and protocols in order to secure and protect LabCorp customers' data.

5. Defendant's intentional, willful, reckless, and/or negligent conduct—failing to prevent the Data Breach, failing to limit its severity, failing to detect it in a timely fashion, and failing to timely notify Plaintiffs and the Class—damaged Plaintiffs and Class Members uniformly. As discussed herein, fraudulent activities have already been linked to Defendant's conduct. For this reason, Defendant should pay for appropriate identity-theft protection services and reimburse Plaintiffs and Class Members for the costs of LabCorp's sub-standard security practices and failure to timely disclose the Data Breach. Plaintiffs and Class Members are, therefore, entitled to injunctive and other equitable relief that safeguards their information, requires Defendant to significantly improve its data security, and provides independent, expert oversight of Defendant's security systems.

JURISDICTION AND VENUE

6. This Consolidated Complaint is intended to serve as an administrative summary as to all other complaints consolidated in this multidistrict litigation asserting claims against LabCorp and shall serve for all purposes as an administrative device to aid efficiency and economy for the Class defined below. As set forth herein, this Court has general jurisdiction over Defendant and original jurisdiction over Plaintiffs' claims.

7. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Defendant is a citizen of a state different from that of at least one Class Member.

8. This Court has personal jurisdiction over LabCorp because it is registered and regularly conducts business in New Jersey and has sufficient minimum contacts in New Jersey such that LabCorp intentionally avails itself of this Court's jurisdiction by conducting operations here and contracts with companies in this District. LabCorp owns and operates many blood testing labs throughout New Jersey and the United States.

9. Venue is proper in this District pursuant to 28 U.S.C. § 1407 and the July 31, 2019 Transfer Order of the Judicial Panel on Multidistrict Litigation in MDL 2904 or, in the alternative, pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this District. Venue is additionally proper because Defendant transacts business and may be found in this District.

NAMED PLAINTIFFS

10. Plaintiffs are individuals who, upon information and belief, had their Personal Information compromised in the Data Breach, and bring this action on behalf of themselves and

all those similarly situated both across the United States and within their state or territory of residence. These allegations are made upon information and belief derived from, *inter alia*, counsel's investigation, public sources – including sworn statements, Defendant's website, and the facts and circumstances currently known. Because Defendant has exclusive but incomplete knowledge of what information was compromised for each individual, including PHI, Plaintiffs reserve the right to supplement their allegations with additional facts and injuries as they are discovered.

ARKANSAS

11. Plaintiff Sherrie Palmer is, and was at all relevant times, a citizen and resident of the State of Arkansas. Plaintiff Palmer utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Palmer's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Palmer received a data breach notification letter from LabCorp. In or around 2018 or 2019, Plaintiff Palmer suffered fraud when unauthorized charges appeared on her credit card account, requiring her to replace her credit card. Since learning of the AMCA data breach, Plaintiff Palmer has taken precautions to mitigate the risk of future identity theft and fraud, including checking her statements for unauthorized activity. To date, Plaintiff Palmer has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Palmer will need to continue indefinitely to protect against fraud and identity theft.

CALIFORNIA

12. Plaintiff Sandra Lassiter is, and was at all relevant times, a citizen and resident of the State of California. Plaintiff Lassiter utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Lassiter's Personal Information to AMCA as

part of its bill collections practice. On or about July 20, 2019, Plaintiff Lassiter received a data breach notification letter from LabCorp. In or around 2018, Plaintiff Lassiter suffered fraud when unauthorized charges appeared on her bank account, requiring her to replace her debit card. Since learning of the AMCA data breach, Plaintiff Lassiter has taken precautions to mitigate the risk of future identity theft and fraud, including spending approximately $60 on password protection software to protect against fraud. To date, Plaintiff Lassiter has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Lassiter will need to continue indefinitely to protect against fraud and identity theft.

13. Plaintiff Aleksandr Nazemnikov is, and was at all relevant times, a citizen and resident of the State of California. Plaintiff Nazemnikov utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Nazemnikov's Personal Information to AMCA as part of its bill collections practice. In or around July 2019, Plaintiff Nazemnikov received a data breach notification letter from LabCorp. In or around the Spring of 2019, Plaintiff Nazemnikov suffered fraud when unauthorized international charges were attempted on his debit card. Since learning of the AMCA data breach, Plaintiff Nazemnikov has taken precautions to mitigate the risk of future identity theft and fraud, including monitoring his accounts for fraudulent activity. To date, Plaintiff Nazemnikov has spent several hours per month checking his credit and financial accounts for any unauthorized activity, a practice Plaintiff Nazemnikov will need to continue indefinitely to protect against fraud and identity theft.

FLORIDA

14. Plaintiff Tracy Buhr is, and was at all relevant times, a citizen and resident of the State of Florida. Plaintiff Buhr utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Buhr's Personal Information to AMCA as part of its bill

collections practice. On or about July 12, 2019, Plaintiff Buhr received a data breach notification letter from LabCorp. Since learning of the AMCA data breach, Plaintiff Buhr has taken precautions to mitigate the risk of future identity theft and fraud, including checking her statements for unauthorized activity. To date, Plaintiff Buhr has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Buhr will need to continue indefinitely to protect against fraud and identity theft.

15. Plaintiff Susan Duckworth is, and was at all relevant times, a citizen and resident of the State of Florida. Plaintiff Duckworth utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Duckworth's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Duckworth received a data breach notification letter from LabCorp. Since learning of the AMCA data breach, Plaintiff Duckworth has taken precautions to mitigate the risk of future identity theft and fraud, including spending approximately $250 on credit monitoring services to protect against fraud. To date, Plaintiff Duckworth has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Duckworth will need to continue indefinitely to protect against fraud and identity theft.

16. Plaintiff Tanya Harris is, and was at all relevant times, a citizen and resident of the State of Florida. Plaintiff Harris utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Harris's Personal Information to AMCA as part of its bill collections practice. On or about June 6, 2019, Plaintiff Harris received a data breach notification letter from AMCA. In or around January 2019, Plaintiff Harris suffered credit card fraud when unauthorized charges were made on her bank account and credit card inquiries were made without her authorization. Since learning of the AMCA data breach, Plaintiff Harris has taken precautions

to mitigate the risk of future identity theft and fraud, including credit monitoring and checking bank statements closely. To date, Plaintiff Harris has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Harris will need to continue indefinitely to protect against fraud and identity theft.

17. Plaintiff Holly Laufenberg is, and was at all relevant times, a citizen and resident of the State of Florida. Plaintiff Laufenberg utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Laufenberg's Personal Information to AMCA as part of its bill collections practice. Plaintiff Laufenberg received collection notices from AMCA related to Plaintiff Laufenberg's LabCorp bill. In or around 2018, during the Data Breach window, Plaintiff Laufenberg suffered fraud when unauthorized charges appeared on her debit card. Since learning of the AMCA data breach, Plaintiff Laufenberg has taken precautions to mitigate the risk of future identity theft and fraud, including obtaining credit monitoring services. To date, Plaintiff Laufenberg has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Laufenberg will need to continue indefinitely to protect against fraud and identity theft.

18. Plaintiff Timothy Petri is, and was at all relevant times, a citizen and resident of the State of Florida. Plaintiff Petri utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Petri's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Petri received a data breach notification letter from LabCorp. In or around November 2018, Plaintiff Petri suffered identity theft when his personal website, email, and other Personal Information on his personal cellphone were erased and made inaccessible. Plaintiff Petri also has received many unsolicited emails since his Personal Information was compromised. Since learning of the AMCA data breach, Plaintiff Petri has taken

precautions to mitigate the risk of future identity theft and fraud, including credit monitoring. To date, Plaintiff Petri has spent several hours per month checking his credit and financial accounts for any unauthorized activity, a practice Plaintiff Petri will need to continue indefinitely to protect against fraud and identity theft.

GEORGIA

19. Plaintiff Jennifer Haley is, and was at all relevant times, a citizen and resident of the State of Georgia. Plaintiff Haley utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Haley's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Haley received a data breach notification letter from LabCorp. Since learning of the AMCA data breach, Plaintiff Haley has taken precautions to mitigate the risk of future identity theft and fraud, including credit monitoring. To date, Plaintiff Haley has spent about several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Haley will need to continue indefinitely to protect against fraud and identity theft.

20. Plaintiff Justin Nelson-Carter is, and was at all relevant times, a citizen and resident of the State of Georgia. Plaintiff Nelson-Carter utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Nelson-Carter's Personal Information to AMCA as part of its bill collections practice. Plaintiff Nelson-Carter received collection notices from AMCA in the spring of 2019 related to Plaintiff Nelson-Carter's LabCorp bill. On or about July 12, 2019, Plaintiff Nelson-Carter received a data breach notification letter from LabCorp. Since learning of the AMCA data breach, Plaintiff Nelson-Carter has taken precautions to mitigate the risk of future identity theft and fraud, including obtaining credit monitoring services and credit freezes. To date, Plaintiff Nelson-Carter has spent about several hours per month checking his

credit and financial accounts for any unauthorized activity, a practice Plaintiff Nelson-Carter will need to continue indefinitely to protect against fraud and identity theft.

21. Plaintiff Valerie Scott is, and was at all relevant times, a citizen and resident of the State of Georgia. Plaintiff Scott utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Scott's Personal Information to AMCA as part of its bill collections practice. On or about July 20, 2019, Plaintiff Scott received a data breach notification letter from LabCorp. In or around October 2019, Plaintiff Scott suffered unauthorized activity on her bank accounts when she received messages from her bank accounts asking to approve transactions she never authorized. Since learning of the AMCA data breach, Plaintiff Scott has taken precautions to mitigate the risk of future identity theft and fraud, including credit monitoring. Plaintiff Scott has spent $15 per month on credit monitoring to protect against fraud. To date, Plaintiff Scott has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Scott will need to continue indefinitely to protect against fraud and identity theft.

KANSAS

22. Plaintiff David Finch is, and was at all relevant times, a citizen and resident of the State of Kansas. Plaintiff Finch utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Finch's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Finch received a data breach notification letter from LabCorp. Since learning of the AMCA data breach, Plaintiff Finch has taken precautions to mitigate the risk of future identity theft and fraud, including reviewing his credit and financial accounts for unauthorized activity. To date, Plaintiff Finch has spent about several

hours per month checking his credit and financial accounts for any unauthorized activity, a practice Plaintiff Finch will need to continue indefinitely to protect against fraud and identity theft.

KENTUCKY

23. Plaintiff George Rothwell is, and was at all relevant times, a citizen and resident of the Commonwealth of Kentucky. Plaintiff Rothwell utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Rothwell's Personal Information to AMCA as part of its bill collections practice. On or about July 20, 2019, Plaintiff Rothwell received a data breach notification letter from LabCorp. Since learning of the AMCA data breach, Plaintiff Rothwell has taken precautions to mitigate the risk of future identity theft and fraud, including credit monitoring. To date, Plaintiff Rothwell has spent several hours per month checking his credit and financial accounts for any unauthorized activity, a practice Plaintiff Rothwell will need to continue indefinitely to protect against fraud and identity theft.

MARYLAND

24. Plaintiff Cassandra Jerry is, and was at all relevant times, a citizen and resident of the State of Maryland. Plaintiff Jerry utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Jerry's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Jerry received a data breach notification letter from LabCorp. Since learning of the AMCA data breach, Plaintiff Jerry has taken precautions to mitigate the risk of future identity theft and fraud, including checking her statements for unauthorized activity. To date, Plaintiff Jerry has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Jerry will need to continue indefinitely to protect against fraud and identity theft.

25. Plaintiff Carol Kaplan is, and was at all relevant times, a citizen and resident of the State of Maryland. Plaintiff Kaplan utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Kaplan's Personal Information to AMCA as part of its bill collections practice. On or about July 20, 2019, Plaintiff Kaplan received a data breach notification letter from LabCorp. Since learning of the AMCA data breach, Plaintiff Kaplan has taken precautions to mitigate the risk of future identity theft and fraud, including checking her statements for unauthorized activity. To date, Plaintiff Kaplan has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Kaplan will need to continue indefinitely to protect against fraud and identity theft.

MASSACHUSETTS

26. Plaintiff Tatyana Shulman is, and was at all relevant times, a citizen and resident of the Commonwealth of Massachusetts. Plaintiff Shulman utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Shulman's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Shulman received a data breach notification letter from LabCorp. In or around May 2019 and June 2019, Plaintiff Shulman suffered fraudulent activity on her credit cards, when unauthorized international and/or online charges appeared on her accounts. Since learning of the AMCA data breach, Plaintiff Shulman has taken precautions to mitigate the risk of future identity theft and fraud, including monitoring her account activity. To date, Plaintiff Shulman has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Shulman will need to continue indefinitely to protect against fraud and identity theft.

MISSISSIPPI

27. Plaintiff Brenda Evans is, and was at all relevant times, a citizen and resident of the State of Mississippi. Plaintiff Evans utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Evans's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Evans received a data breach notification letter from LabCorp. Since learning of the AMCA data breach, Plaintiff Evans has taken precautions to mitigate the risk of future identity theft and fraud, including checking her statements for unauthorized activity. To date, Plaintiff Evans has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Evans will need to continue indefinitely to protect against fraud and identity theft.

28. Plaintiff Cameron Spencer is, and was at all relevant times, a citizen and resident of the State of Mississippi. Plaintiff Spencer utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Spencer's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Spencer received a data breach notification letter from LabCorp. In or around August 2019, Plaintiff Spencer suffered identity theft when he received checks under his name and address from a place at which he is not employed. Plaintiff Spencer also received credit card inquiries he did not authorize. Since learning of the AMCA data breach, Plaintiff Spencer has taken precautions to mitigate the risk of future identity theft and fraud, including credit monitoring and checking his bank account activity. To date, Plaintiff Spencer has spent several hours per month checking his credit and financial accounts for any unauthorized activity, a practice Plaintiff Spencer will need to continue indefinitely to protect against fraud and identity theft.

29. Plaintiff Kristopher Thomas is, and was at all relevant times, a citizen and resident of the State of Mississippi. Plaintiff Thomas utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Thomas's Personal Information to AMCA as part of its bill collections practice. On or about July 26, 2019, Plaintiff Thomas received a data breach notification letter from LabCorp. In or around early 2019, Plaintiff Thomas had a fraudulent transaction of approximately $200 on his debit card. Plaintiff Thomas also received an email that his Personal Information was on the dark web. Since learning of the AMCA data breach, Plaintiff Thomas has taken precautions to mitigate the risk of future identity theft and fraud, including checking his statements for unauthorized activity. To date, Plaintiff Thomas has spent several hours per month checking his credit and financial accounts for any unauthorized activity, a practice Plaintiff Thomas will need to continue indefinitely to protect against fraud and identity theft.

NEW JERSEY

30. Plaintiff Jesse Lebon is, and was at all relevant times, a citizen and resident of the State of New Jersey. Plaintiff Lebon utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Lebon's Personal Information to AMCA as part of its bill collections practice. Plaintiff Lebon received collection notices from AMCA in the spring of 2019 related to Plaintiff Lebon's LabCorp bill. Since learning of the AMCA data breach, Plaintiff Lebon has taken precautions to mitigate the risk of future identity theft and fraud, including checking his accounts for unauthorized activity. To date, Plaintiff Lebon has spent several hours per month checking his credit and financial accounts for any unauthorized activity, a practice Plaintiff Lebon will need to continue indefinitely to protect against fraud and identity theft.

NEW YORK

31. Plaintiff Rosaria Gadero is, and was at all relevant times, a citizen and resident of the State of New York. Plaintiff Gadero utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Gadero's Personal Information to AMCA as part of its bill collections practice. On or about July 20, 2019, Plaintiff Gadero received a data breach notification letter from LabCorp. On or about June 6, 2019, Plaintiff Gadero received a data breach notification letter from AMCA. In or around May 2019, Plaintiff Gadero suffered fraudulent activity on her bank account three times. Since learning of the AMCA data breach, Plaintiff Gadero has taken precautions to mitigate the risk of future identity theft and fraud, including credit monitoring and checking bank activities closely. To date, Plaintiff Gadero has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Gadero will need to continue indefinitely to protect against fraud and identity theft.

32. Plaintiff Lori Lamondie-Murphy is, and was at all relevant times, a citizen and resident of the State of New York. Plaintiff Lamondie-Murphy utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Lamondie-Murphy's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Lamondie-Murphy received a data breach notification letter from LabCorp. In or around 2018, Plaintiff Lamondie-Murphy suffered identity theft when someone attempted to open accounts in her name without authorization. Since learning of the AMCA data breach, Plaintiff Lamondie-Murphy has taken precautions to mitigate the risk of future identity theft and fraud, including monitoring her credit and financial accounts. To date, Plaintiff Lamondie-Murphy has spent several hours per month checking her credit and financial accounts for any unauthorized activity,

a practice Plaintiff Lamondie-Murphy will need to continue indefinitely to protect against fraud and identity theft.

33. Plaintiff Wendy Wallach is, and was at all relevant times, a citizen and resident of the State of New York. Plaintiff Wallach utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Wallach's Personal Information to AMCA as part of its bill collections practice. On or about June 6, 2019, Plaintiff Wallach received a data breach notification letter from AMCA. Since learning of the AMCA data breach, Plaintiff Wallach has taken precautions to mitigate the risk of future identity theft and fraud, including monitoring her credit monitoring services for unauthorized activity. After learning of the AMCA data breach, Plaintiff Wallach has received notifications from her credit monitoring services that her Personal Information was found on the dark web. To date, Plaintiff Wallach has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Wallach will need to continue indefinitely to protect against fraud and identity theft.

NORTH CAROLINA

34. Plaintiff Melanie Vazquez is, and was at all relevant times, a citizen and resident of the State of North Carolina. Plaintiff Vazquez utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Vazquez's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Vazquez received a data breach notification letter from LabCorp. In or around September 2018 and December 2018, Plaintiff Vazquez had two fraudulent transactions on her credit cards. Plaintiff Vazquez later received a replacement credit card in the mail with the fraudulent user's name on the card. Plaintiff Vazquez spent numerous hours resolving these fraudulent charges, including placing a freeze on her credit in or around December 2018. Since learning of the AMCA data breach, Plaintiff

Vazquez has taken precautions to mitigate the risk of future identity theft and fraud, including checking her credit statements for unauthorized activity. To date, Plaintiff Vazquez has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Vazquez will need to continue indefinitely to protect against fraud and identity theft.

35. Plaintiff Debra Wrenn is, and was at all relevant times, a citizen and resident of the State of North Carolina. Plaintiff Wrenn utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Wrenn's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Wrenn received a data breach notification letter from LabCorp. In or around July 30, 2019, Plaintiff Wrenn suffered fraud when there was a credit card inquiry in her name that she did not authorize. Since learning of the AMCA data breach, Plaintiff Wrenn has taken precautions to mitigate the risk of future identity theft and fraud, including credit monitoring and credit freeze. To date, Plaintiff Wrenn has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Wrenn will need to continue indefinitely to protect against fraud and identity theft.

OHIO

36. Plaintiff Sheera Harris is, and was at all relevant times, a citizen and resident of the State of Ohio. Plaintiff Harris utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Harris's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Harris received a data breach notification letter from LabCorp. Since learning of the AMCA data breach, Plaintiff Harris has taken precautions to mitigate the risk of future identity theft and fraud, including credit monitoring and

credit freeze. To date, Plaintiff Harris has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Harris will need to continue indefinitely to protect against fraud and identity theft.

37. Plaintiff Edith Thrower is, and was at all relevant times, a citizen and resident of the State of Ohio. Plaintiff Thrower utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Thrower's Personal Information to AMCA as part of its bill collections practice. On or about July 20, 2019, Plaintiff Thrower received a data breach notification letter from LabCorp. In or around early 2019, Plaintiff Thrower suffered fraud when she learned of many credit account inquiries she did not authorize. Since learning of the AMCA data breach, Plaintiff Thrower has taken precautions to mitigate the risk of future identity theft and fraud, including checking statements thoroughly. To date, Plaintiff Thrower has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Thrower will need to continue indefinitely to protect against fraud and identity theft.

OKLAHOMA

38. Plaintiff Isaac Williams-Winters is, and was at all relevant times, a citizen and resident of the State of Oklahoma. Plaintiff Williams-Winters previously resided in Florida. Plaintiff Williams-Winters utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Williams-Winters's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 2019, Plaintiff Williams-Winters received a data breach notification letter from LabCorp. Since learning of the AMCA data breach, Plaintiff Williams-Winters has taken precautions to mitigate the risk of future identity theft and fraud, including credit monitoring. To date, Plaintiff Williams-Winters has spent several hours per month

checking his credit and financial accounts for any unauthorized activity, a practice Plaintiff Williams-Winters will need to continue indefinitely to protect against fraud and identity theft.

PENNSYLVANIA

39. Plaintiff Timothy Judelsohn is, and was at all relevant times, a citizen and resident of the Commonwealth of Pennsylvania. Plaintiff Judelsohn utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Judelsohn's Personal Information to AMCA as part of its bill collections practice. On or about July 20, 2019, Plaintiff Judelsohn received a data breach notification letter from LabCorp. In or around August 2019, Plaintiff Judelsohn suffered identity theft when one of his credit cards was cloned in his name without his authorization. Since learning of the AMCA data breach, Plaintiff Judelsohn has taken precautions to mitigate the risk of future identity theft and fraud, including monitoring his credit and financial accounts. To date, Plaintiff Judelsohn has spent several hours per month checking his credit and financial accounts for any unauthorized activity, a practice Plaintiff Judelsohn will need to continue indefinitely to protect against fraud and identity theft.

TENNESSEE

40. Plaintiff Tiffany Goins is, and was at all relevant times, a citizen and resident of the State of Tennessee. Plaintiff Goins utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Goins's Personal Information to AMCA as part of its bill collections practice. On or about June 4, 2019, Plaintiff Goins received a data breach notification letter from AMCA. In or around October 2018, Plaintiff Goins suffered identity theft when there was a credit card account inquiry Plaintiff Goins did not authorize. Since learning of the AMCA data breach, Plaintiff Goins has taken precautions to mitigate the risk of future identity theft and fraud, including credit monitoring and credit freeze. Plaintiff Goins has spent $30 per month on

credit monitoring to protect against fraud. To date, Plaintiff Goins has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Goins will need to continue indefinitely to protect against fraud and identity theft.

TEXAS

41. Plaintiff Martha Cuvillier is, and was at all relevant times, a citizen and resident of the State of Texas. Plaintiff Cuvillier utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Cuvillier's Personal Information to AMCA as part of its bill collections practice. On or about July 26, 2019, Plaintiff Cuvillier received a data breach notification letter from LabCorp. To date, Plaintiff Cuvillier has spent several hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Cuvillier will need to continue indefinitely to protect against fraud and identity theft.

WISCONSIN

42. Plaintiff Gina Allende is, and was at all relevant times, a citizen and resident of the State of Wisconsin. Plaintiff Allende utilized the laboratory services of LabCorp and, on information and belief, LabCorp provided Plaintiff Allende's Personal Information to AMCA as part of its bill collections practice. Plaintiff Allende received a collection notice from AMCA in or around November 2018 related to Plaintiff Allende's LabCorp bill. Since learning of the AMCA data breach, Plaintiff Allende has taken precautions to mitigate the risk of future identity theft and fraud, including monitoring her accounts for fraud. To date, Plaintiff Allende has spent several of hours per month checking her credit and financial accounts for any unauthorized activity, a practice Plaintiff Allende will need to continue indefinitely to protect against fraud and identity theft.

DEFENDANT

43. Defendant Laboratory Corporation of America Holdings is a corporation existing under the laws of the State of Delaware with its headquarters and principal place of business located in Burlington, North Carolina.

FACTUAL ALLEGATIONS

A. Labcorp Obtained Personal Information From Plaintiffs And Class Members And Shared That Information With AMCA

44. LabCorp is one of the world's leading providers of medical diagnostic testing services for patient care. Their medical tests aid in the detection, diagnosis, and analysis of disease. For these and other services, LabCorp generated revenues of approximately $11.3 billion in 2018.

45. LabCorp offers a variety of clinical laboratory testing services to patients, including Plaintiffs and Class Members, following a referral from a physician. As of February 2019, LabCorp stated that it processes "2.5 million patient specimens each week and has laboratory locations throughout the U.S."[2]

46. LabCorp offers hundreds of different tests "used in general patient care by physicians to establish or support a diagnosis, to monitor treatment or to search for an otherwise undiagnosed condition."[3] LabCorp's "most frequently requested tests include blood chemistry analyses, urinalyses, blood cell counts, thyroid tests, Pap tests, hemoglobin A1C, prostate-specific antigen (PSA), tests for sexually-transmitted diseases, hepatitis C (HCV), tests, vitamin D,

---

[2] LabCorp Form 10-K at 7 (Feb. 28, 2019), https://www.sec.gov/Archives/edgar/data/920148/000092014819000033/lh10-k2018.htm.

[3] *Id.* at 9.

microbiology cultures and procedures, and alcohol and other substance-abuse tests."[4] LabCorp performs this core group of tests in its major laboratories.[5]

47. LabCorp operates a network of "Patient Service Centers" ("PSCs") throughout the U.S., at which it performs specimen collection services for patients, such as Plaintiffs and Class Members.[6] Its PSC staff, generally phlebotomists, collects specimens for testing as requested by the ordering physician. Additionally, "[a] significant portion of patient specimens are collected by [healthcare providers'] staff at its office or facility, or in some cases, by a [LabCorp] phlebotomist who has been placed in the PSC location for the specific purpose of collecting and processing specimens to be tested by [LabCorp]."[7]

48. For appointments at its PSCs, LabCorp requires patients, such as Plaintiffs and Class Members, to bring with them and provide to LabCorp a LabCorp test request form or prescription from the healthcare professional requesting the laboratory testing; a current insurance identification card (Medicare, private insurance or HMO/PPO); a photo ID; and a health spending account card, credit card, or debit card.[8]

49. LabCorp promises that its "staff will make the specimen collection process as safe, quick, and comfortable as possible while safeguarding your dignity and privacy."[9]

---

4 *Id*.

5 *Id*.

6 *Id*. at 5.

7 *Id*. at 8.

8 What to Expect, LabCorp, https://www.labcorp.com/labs-and-appointments/what-to-expect (last visited June 10, 2019).

9 *Id.*

50. LabCorp charges for the laboratory services it provides to patients, including Plaintiffs and Class Members. If the patient does not have insurance, or if the insurance does not cover the clinical laboratory testing services, the patient is responsible for paying for the full amount of the services performed.[10]

51. LabCorp generates bills for its patients, including for Plaintiffs and Class Members. Accounts receivable are then monitored by LabCorp billing personnel and follow-up activities are conducted as necessary.[11]

52. LabCorp refers unpaid bills to a collection agency. AMCA is an external collection agency LabCorp utilized to collect unpaid bills. LabCorp has referred more than 10.2 million patients, including Plaintiffs and Class Members, to AMCA.[12] AMCA is a "business associate" of LabCorp under The Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

53. LabCorp provided AMCA with Personal Information regarding LabCorp's patients in order to facilitate the bill-collection process. These patients' data was stored in the AMCA systems that were compromised by the Data Breach.[13]

54. The patient information LabCorp provided to AMCA, including Plaintiffs' and Class Members', included personal and medical information, such as the first and last name, date

---

[10] *See Frequently Asked Questions: Billing & Insurance, LabCorp,* https://www.labcorp.com/frequently-asked-questions/patient/11/all/ (last visited June 10, 2019).

[11] LabCorp Form 10-K at 12 (Feb. 28, 2019), https://www.sec.gov/Archives/edgar/data/920148/000092014819000033/lh10-k2018.htm.

[12] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,* U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited October 9, 2019).

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

of birth, address, telephone number, date of service, service provider, and account balance information.[14]

55. AMCA collects and maintains the information LabCorp provided to AMCA in its own computer systems. These same AMCA systems were compromised in the Data Breach.

56. In addition, AMCA also obtains Personal Information from the LabCorp patients from whom AMCA seeks to collect payments on LabCorp's behalf. This information includes financial information, such as credit card or bank account information. Upon information and belief, AMCA stored this information in the computer systems compromised in the Data Breach.

57. In U.S. Bankruptcy Court in the Southern District of New York, AMCA has admitted that its "business, by its very nature, requires it to collect and maintain data transmitted to it by its clients [such as LabCorp] that includes personally identifiable information about third-party debtors that could include names, home addresses, social security numbers, bank account information for consumers choosing to pay online by check and, for consumers choosing to pay their outstanding balances by credit card, credit card information." AMCA has also admitted that this "information might also include dates of birth and certain medical information related to any laboratory tests for which payment is sought."[15]

---

[14] *Id.*; *see also In re Retrieval-Masters Creditors Bureau, Inc.*, No. 7:19-bk-23185, Dkt. No. 2 (Bankr. S.D.N.Y. Jun 17, 2019).

[15] Declaration of Russell H. Fuchs Pursuant to Local Bankruptcy Rule 1007-2 and in Support of "First Day" Motions, *In re Retrieval-Masters Creditors Bureau, Inc.*, No. 19-23185-RDD (Bankr. S.D.N.Y. June 17, 2019), ECF No. 2 at 4-5.

B. The Data Breach

58. Between August 1, 2018 and March 30, 2019, an unauthorized user or users gained access to the AMCA system that contained information obtained from various entities, including Defendant LabCorp, as well as information that AMCA collected itself.

59. More than 10.2 million LabCorp patients have been affected by the Data Breach, which is the second-largest breach, following the breach of Quest patients' data, reported to the U.S. Department of Health and Human Services ("HHS") in 2019.[16] LabCorp's Data Breach was also the second -largest to be reported since HHS's Office for Civil Rights launched its breach portal in 2010.[17]

60. On February 28, 2019, Gemini Advisory identified a large number of compromised payment cards while monitoring dark-web marketplaces where payment card data, and associated PII, is bought and sold. Almost 15% of these records of compromised payment cards included additional PII, such as dates of birth, Social Security numbers, and physical addresses. A thorough analysis indicated that the information was likely stolen from the unsecure online portal of AMCA.

---

[16] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,* U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited October 9, 2019); *see also August 2019 Healthcare Data Breach Report*, HIPAA Journal, https://www.hipaajournal.com/august-2019-healthcare-data-breach-report/ (last visited October 9, 2019).

[17] *July-reported healthcare breaches exposed 22 million people's data*, Modern Healthcare, https://www.modernhealthcare.com/cybersecurity/july-reported-healthcare-breaches-exposed-22-million-peoples-data (last visited October 9, 2019).

Several financial institutions also collaboratively confirmed the connection between the compromised payment card data and the breach at AMCA.[18]

61. "On March 1, 2019, Gemini Advisory attempted to notify AMCA," but as Gemini Advisory reportedly told DataBreaches.net, "they did not get any response to phone messages they left." Failing to obtain any response from AMCA, Gemini Advisory "promptly contacted federal law enforcement, which reportedly followed up by contacting AMCA."[19]

62. Following notification from law enforcement, AMCA's payment portal became unavailable for weeks.[20]

63. On May 14, 2019, AMCA notified LabCorp that there was a Data Breach of AMCA's web payment page. In response to AMCA's initial notification of the Data Breach, LabCorp indicated it would cease sending new collection requests to AMCA and had told AMCA to stop work on any pending collection requests involving LabCorp customers.[21]

64. In a written statement attributed to AMCA, AMCA announced it is still investigating the breach:

> "We are investigating a data incident involving an unauthorized user accessing the American Medical Collection Agency system," reads a written statement attributed to the AMCA. "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.
> . . . .

---

[18] *American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory*, DataBreaches.net (May 10, 2019), *available at* https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/.

[19] *Id.*

[20] *Id.*

[21] *Information about the AMCA Data Security Incident*, LabCorp, https://www.labcorp.com/AMCA-data-security-incident (last updated June 10, 2019).

> We hired a third-party external forensics firm to investigate any potential security breach in our systems, migrated our web payments portal services to a third-party vendor, and retained additional experts to advise on, and implement, steps to increase our systems' security. We have also advised law enforcement of this incident. We remain committed to our system's security, data privacy, and the protection of personal information."[22]

65. LabCorp should have known of the Data Breach no later than March 2019. However, LabCorp did not take any steps to notify the public – much less directly notify patients whose information was affected – until June 4, 2019, when LabCorp informed its investors of the Data Breach through an SEC filing.

66. LabCorp announced in its June 4, 2019 filing with the SEC:

> [LabCorp] has been notified by Retrieval-Masters Creditors Bureau, Inc. d/b/a American Medical Collection Agency (AMCA) about unauthorized activity on AMCA's web payment page (the AMCA Incident). According to AMCA, this activity occurred between August 1, 2018, and March 30, 2019. AMCA is an external collection agency used by LabCorp and other healthcare companies. LabCorp has referred approximately 7.7 million consumers to AMCA whose data was stored in the affected AMCA system. AMCA's affected system included information provided by LabCorp. That information could include first and last name, date of birth, address, phone, date of service, provider, and balance information. AMCA's affected system also included credit card or bank account information that was provided by the consumer to AMCA (for those who sought to pay their balance).[23]

67. LabCorp further disclosed in its June 4, 2019 SEC filing that "AMCA has informed LabCorp that it is in the process of sending notices to approximately 200,000 LabCorp consumers whose credit card or bank account information may have been accessed. AMCA has not yet

---

[22] *LabCorp: 7.7 Million Consumers Hit in Collections Firm Breach, Krebs on Security* (June 4, 2019), https://krebsonsecurity.com/2019/06/labcorp-7-7m-consumers-hit-in-collections-firm-breach/; *see also Information about the AMCA Data Security Incident*, LabCorp, https://www.labcorp.com/AMCA-data-security-incident (last updated June 10, 2019).

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

provided LabCorp a list of the affected LabCorp consumers or more specific information about them."[24]

68. While LabCorp's June 4, 2019 SEC filing stated that "AMCA has advised LabCorp that Social Security Numbers and insurance identification information are not stored or maintained for LabCorp consumers,"[25] LabCorp later disclosed that Social Security Numbers and health insurance information may have been included as well.[26]

69. LabCorp announced in its August 8, 2019 filing with the SEC:

> Information on AMCA's affected system from the Company may have included name, address, and balance information for the patient and person responsible for payment, along with the patient's phone number, date of birth, referring physician, and date of service. **The Company was later informed by AMCA that health insurance information may have been included for some individuals, and because some insurance carriers utilize the Social Security Number as a subscriber identification number, the Social Security Number for some individuals may also have been affected.** [27]

---

24 *Id*.

25 *Id*.

26 LabCorp Form 8-K (August 8, 2019), https://www.sec.gov/ix?doc=/Archives/edgar/data/920148/000092014819000076/lh201910-qq2.htm.

27 *Id.* (emphasis added).

70. On or about July 13, 2019, LabCorp disclosed to the Office for Civil Rights that 10,251,784 individuals have been affected by the Data Breach.[28] LabCorp did not disclose this fact either in its August 8, 2019 filing with the SEC or on its website.[29]

C. Labcorp Failed To Exercise Due Care In Contracting With AMCA

71. LabCorp failed to exercise due care in protecting patients' information by contracting with AMCA to handle its debt collections.

72. AMCA's bankruptcy filings indicate how thinly capitalized the company was and how insignificant its information technology ("IT") department and infrastructure were. Public reporting has highlighted that AMCA was not a reputable business associate – let alone an associate to be trusted with Plaintiffs' and Class Members' Personal Information.

73. Specifically, AMCA's bankruptcy filings admit that it had less than $4 million in liquidity and its owner had to take a secured loan from his own personal funds simply to mail notices to those impacted by the Data Breach. Put simply, LabCorp should not have contracted with an entity that did not even have the means to mail notices to people without having to file for bankruptcy.

74. The length of time between the breach and AMCA's claimed discovery of the breach indicates that AMCA's systems to detect intrusion, detect unusual activity, and log and

---

[28] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,* U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited October 9, 2019).

[29] *See* LabCorp Form 8-K (August 8, 2019), https://www.sec.gov/ix?doc=/Archives/edgar/data/920148/000092014819000076/lh201910-qq2.htm (emphasis added); *see also Laboratory Corporation of America Holdings Notice Regarding AMCA Security Incident*, LabCorp, https://www.labcorp.com/AMCA-data-security-incident (last updated September 13, 2019).

report such events were woefully inadequate and not in compliance with industry standards. For example, according to technology-security company FireEye, the median amount of time between when a data breach occurs and when it is detected was 78 days in 2018. This number has consistently been trending downward in recent years due to improvements in detection technology.[30] The fact that it took AMCA 242 days to detect the Data Breach, nearly 3.5 times the median time for detection in 2018, is direct evidence of its failure to employ reasonable, industry-standard data security practices to safeguard Plaintiffs' and Class Members' Personal Information. AMCA's data security deficiencies would have been readily apparent to LabCorp had LabCorp adequately investigated AMCA's capabilities (or lack thereof).

75. AMCA's inability to detect its own Data Breach, when an unrelated security firm (Gemini Advisory – which was not working for AMCA) was apparently able to do so with ease, is further evidence of the fact that AMCA employed inadequate data security practices, and that LabCorp failed in its independent obligation to ensure that its HIPAA business associate employed reasonable and industry-standard data security measures. The FireEye report indicates that in 2018, the median amount of time that it took a third party to detect a data breach was three times the median time for internal detection.[31]

76. Some of the easiest ways to minimize exposure to a data breach are to limit the type and amount of information provided to business associates, and routine destruction or archiving of inactive PII and PHI so that it cannot not be accessed through online channels. Access to the 10.2 million LabCorp patient records through AMCA's online portal should not have been possible,

---

[30] *M-Trends 2019: FireEye Mandiant Services Special Report, available at* https://content.fireeye.com/m-trends (last visited June 11, 2019).

[31] *Id.*

had AMCA maintained appropriate protections. The sheer number of records suggests that AMCA was not destroying or archiving inactive records. Again, LabCorp would have discovered this had it exercised adequate oversight over its business associates and audited the data security protocols utilized by AMCA.

77. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). AMCA was not encrypting payment card information according to minimum industry standards established in PCI DSS.

78. The payment card industry has published a guide on point-to-point encryption and its benefits in securing payment card data: "point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[32]

79. Had AMCA implemented a P2PE solution prior to the Data Breach and the Data Breach occurred, that data would have been commercially worthless to the attacker as the attacker would not have been able to decrypt the data to obtain the information necessary to make fraudulent purchases. Gemini found credit card numbers from the Data Breach for sale on the dark web, which means that AMCA did not encrypt those numbers in accordance with PCI DSS.

---

[32] *Securing Account Data with the PCI Point –to-Point Encryption Standard v2*, available at https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf (last accessed June 11, 2019).

80. LabCorp had an obligation to exercise oversight over AMCA in a manner that would include immediate knowledge of any data security incidents experienced by AMCA that could affect LabCorp's patients. For example, AMCA pointed to the fact that it learned of the unauthorized access in March 2019 through a series of CPP notices suggesting that a "disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges."[33] However, LabCorp did not learn of the unauthorized access until months later in May 2019.

D. Labcorp Failed To Provide Proper Notice Of The Data Breach

81. Although LabCorp was on notice of the Data Breach on May 14, 2019 (and should have known months earlier), it took LabCorp **21** days to publicly acknowledge the Breach and months longer to provide notice to impacted customers.

82. On June 4, 2019, LabCorp publicly acknowledged the Data Breach and indicated that it would be "working closely with AMCA to obtain more information and to take additional steps as may be appropriate once more is known about the AMCA Incident."[34]

83. However, rather than send notice directly, LabCorp relied on AMCA to mail notices to those individuals on its system in June 2019.[35] The notices provided by AMCA were deficient in several respects. First, AMCA's notices failed to indicate to LabCorp's customers that it was LabCorp who had given their information to AMCA. Thus, many affected individuals were

---

[33] CPP stands for "common point of purchase." CPP analysis identifies the likely source of stolen card numbers so that banks can mitigate future fraud on all cards stolen from that source.

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

[35] *Id.*; Neither AMCA nor LabCorp were prepared to deal with the fallout from, and accept responsibility for, the Data Breach, which is underscored by the fact that a multi-billion dollar business, LabCorp, relied on undercapitalized AMCA to send out the breach notices.

left to guess why AMCA had their Personal Information in the first instance. Additionally, the notices failed to inform LabCorp's customers exactly what information was breached, thus preventing them from taking measures that could possibly prevent further harm.

84. It was not until July 13, 2019, almost four months after AMCA received CPP notices and one month after LabCorp's first public statement, that LabCorp put detailed information on its own website regarding the Data Breach.[36] But even this more detailed notice was deficient in many respects.

a. First, the website indicated that AMCA was the party responsible for sending notice and does not detail any oversight taken by LabCorp over its business associate.

b. Second, the website limits the offer of twenty-four months of complimentary credit monitoring, to those persons whose Social Security numbers may have been affected.[37] This limitation means that customers who had other forms of Personal Information taken are not protected. As detailed *infra*, the theft of various forms of Personal Information, not just Social Security numbers, credit card information, and bank account numbers, can lead to identity theft.

c. Third, LabCorp acknowledges that it may have out-of-date contact information for some of its customers. However, LabCorp provided no means for these customers to obtain information about whether they had been breached and to access credit

---

[36] *Laboratory Corporation of America Holdings Notice Regarding AMCA Security Incident*, LabCorp, https://www.labcorp.com/AMCA-data-security-incident (last updated September 13, 2019).

[37] *Id.*

monitoring. For example, LabCorp's website does not have any information that its customers can use to determine whether their information was part of the Data Breach.

d. Fourth, LabCorp's website offered a toll-free number to allow individuals to ask questions and gather additional information.[38] However, the toll-free number is no longer in service. In addition, (i) the website provides no information about what questions or additional information can be asked or learned and (ii) the phone number is buried in the website's text, without any emphasis.

e. Fifth, the website provides no information about the credit monitoring that LabCorp purported to offer. Rather, it appears to have only been included in some of the mailings and there is no indication to LabCorp's customers on LabCorp's website of how to sign up for this service or any other relevant details.

85. LabCorp sent out letters to customers potentially affected by the breach. These, similarly, provided deficient notice, failing to alert customers as to exactly what information was breached preventing them from taking measures that could possibly prevent further harm.

86. In sum, LabCorp's failure to properly disseminate notice further harmed its customers by keeping them in the dark about whether they were breached, how they could quickly and safely respond, and about what information was vulnerable because of the Data Breach.

E. LabCorp's Duty To Properly Secure Plaintiffs And Class Members' Personal Information

87. LabCorp agreed, and had a continuing contractual and common-law duty and obligation, to keep confidential the Personal Information its patients disclosed to it and to protect this information from unauthorized disclosure. LabCorp's agreements, duties, and obligations are

[38] *Id.*

based on: (1) HIPAA; (2) industry standards; (3) the agreements and promises made to Plaintiffs and Class Members; and (4) Section 5(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Class Members provided their Personal Information to LabCorp with the reasonable belief that LabCorp and its business associates would comply with its agreements and any legal requirements to keep that Personal Information confidential and secure from unauthorized disclosure.

88. HIPAA requires that LabCorp provide every patient it treats, including Plaintiffs and Class Members, with a privacy notice.

89. In this HIPAA-mandated privacy notice, LabCorp agrees that it will keep PHI of its patients, including Plaintiffs and Class Members, confidential and protected from unauthorized disclosure. In its Notice of Privacy Practices effective May 9, 2016, LabCorp promises and agrees in relevant part[39]:

> LabCorp is required by law to maintain the privacy of health information that identifies you, called protected health information (PHI), and to provide you with notice of our legal duties and privacy practices regarding PHI. LabCorp is committed to the protection of your PHI and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation. We take this commitment seriously and will work with you to comply with your right to receive certain information under HIPAA.
>
> * * *
>
> Business associates - LabCorp may disclose PHI to its business associates to perform certain business functions or provide certain business services to LabCorp. For example, we may use another company to perform billing services on our behalf. All of our business associates are required to maintain the privacy and confidentiality of your PHI. In addition, at the request of your health care providers or health plan, LabCorp may disclose PHI to their business associates for purposes of performing certain business functions or health care services on their behalf. For

[39] *HIPAA Information,* LabCorp, https://www.labcorp.com/hipaa-privacy/hipaa-information (last visited October 3, 2019).

> example, we may disclose PHI to a business associate of Medicare for purposes of medical necessity review and audit.

90. LabCorp posts this Notice of Privacy Practices on its website, acknowledging its agreement, duty and promise to protect all PHI in its possession. LabCorp also provides a HIPAA privacy notice to patients at the time of collection.

91. LabCorp promises patients that it will keep their Personal Information confidential, assuring patients that patients' financial "information *may be accessed only by LabCorp employees who maintain password and job-required access rights, and third party vendors who support LabCorp's billing operations*. Additionally, LabCorp maintains all personal patient data within the LabCorp information system (IS) firewalls that operate on separate LabCorp mainframes/servers. *The general public may not access these mainframes/servers.*"[40]

92. LabCorp's data security agreements, obligations, and commitments are particularly important given the substantial increase in data breaches (particularly in the healthcare industry) during the period preceding the Data Breach. LabCorp's failure to provide the data-security protections it committed to provide to Plaintiffs and Class Members was particularly egregious in light of specific government warnings regarding the possibility of attempts to illegally access the data of companies like LabCorp. Such warnings alerted LabCorp to the risk of a data breach and further emphasized LabCorp's duty to keep patients' Personal Information secure and to ensure that its business associates, such as AMCA, kept its patients' Personal Information secure, as HIPAA mandates.

---

[40] *Website Privacy Policy*, LabCorp, https://www.labcorp.com/hipaa-privacy/web-privacy-policy (emphasis added.) (last visited Oct. 3, 2019).

93. As alleged above, AMCA was a "business associate" of LabCorp with whom LabCorp shared Personal Information of LabCorp's patients. Indeed, LabCorp was one of AMCA's two largest clients. As LabCorp's business associate, AMCA was required to maintain the privacy and security of Plaintiffs' and Class Members' Personal Information. HIPAA mandates that a covered entity (*i.e.*, LabCorp) may only disclose PHI to a "business associate" (*i.e.*, AMCA) if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[41] LabCorp failed to ensure that its business associate AMCA safeguarded Personal Information of LabCorp's patients and that AMCA complied with HIPAA's privacy mandates.

F. LabCorp Violated HIPAA's Requirements To Safeguard Data

94. LabCorp had a non-delegable duty to ensure that all information it collected and stored was secure, and that any associated entities with whom they shared member information maintained adequate and commercially-reasonable data security practices to ensure the protection of plan members' Personal Information.

95. LabCorp is covered by HIPAA (*see* 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

[41] *See* 45 CFR §§ 164.502(e), 164.504(e), 164.532(d) and (e).

96. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

97. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

98. HIPAA requires that Defendant implement appropriate safeguards for this information.

99. HIPAA further mandates that a covered entity such as Defendant may disclose PHI to a "business associate," such as AMCA, only if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[42]

100. HIPAA requires that Defendant provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons – *i.e.* non-encrypted data.

101. Despite these requirements, Defendant failed to comply with its duties under HIPAA and its own Privacy Practices. Indeed, Defendant failed to:

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

---

42 *See* 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e).

b. Adequately protect Plaintiffs' and the Class Members' Personal Information;

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

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

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

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

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

h. Take safeguards to ensure that Defendant's business associates adequately protect protected health information;

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

j. Train all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for

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

102. Defendant failed to comply with its duties under HIPAA and its own Codes of Conduct and Privacy Policies despite being aware of the risks associated with unauthorized access of members' Personal Information.

G. LabCorp Was On Notice That Highly Valuable Personal Information Of Its Patients Could Be Breached

103. LabCorp was, or should have been, aware that it was collecting highly valuable data, for which LabCorp knew, or should have known, there is an upward trend in data breaches in recent years.[43] Accordingly, LabCorp was on notice for the harms that could ensue if it failed to protect its patients' data.

104. HHS' Office for Civil Rights currently lists 550 breaches affecting 500 or more individuals in the past 24 months.[44] LabCorp patients are the second largest group, following the Quest patients, damaged by this Data Breach.[45]

105. As early as 2014, the FBI alerted the healthcare industry that it was an increasingly preferred target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or

---

[43] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited September 27, 2019) ("Our healthcare statistics clearly show there has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published.").

[44] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,* U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited October 9, 2019).

[45] *Id.*

Personally Identifiable Information (PII)" so that these companies can take the necessary precautions to thwart such attacks.[46]

106. The co-founder of Lastline, a network security provider, said that "[h]ackers target financial companies, like this billing collection company, as they often store sensitive financial information that can be turned into immediate gains."[47]

107. At the end of 2018, the healthcare sector ranked second-highest in the number of data breaches among measured sectors, and had the highest rate of exposure for each breach.[48] With this Data Breach, 2019 has seen the exposure of three times the number of records compromised in 2018.[49]

108. Other experts have stated that the Data Breach is at "the intersection of three of the types of data that hackers most desire: personal identifying information that can be used for identity fraud, information about medical conditions, and financial account information."[50]

---

[46] Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited September 27, 2019).

[47] Christopher Rowland, *Quest Diagnostics discloses breach of patient records*, WASH. POST, June 3, 2019, https://www.washingtonpost.com/business/economy/quest-diagnostics-discloses-breach-of-patient-records/2019/06/03/aa37b556-860a-11e9-a870-b9c411dc4312_story.html?utm_term=.78dd30c03a88 (last visited September 27, 2019).

[48] *2018 End-of-Year Data Breach Report*, Identity Theft Resource Center, https://www.idtheftcenter.org/2018-data-breaches (last visited April 21, 2019).

[49] *Healthcare Data Breach Statistics* (August 2019), HIPPAA Journal, https://www.hipaajournal.com/august-2019-healthcare-data-breach-report (last visited September 27, 2019).

[50] Scott Ikeda, *Third Party Data Breach Hits Quest Diagnostics with 12 Million Confidential Patient Records Exposed*, CPO Magazine, June 11, 2019, https://www.cpomagazine.com/cyber-security/third-party-data-breach-hits-quest-diagnostics-with-12-million-confidential-patient-records-exposed/ (last visited Oct. 7, 2019).

109. This same article has asked: "why did a collections agency have all of this information in the first place?" It also questioned why medical information and Social Security Numbers needed to be provided to debt collectors.[51]

110. Further, Cathy Allen, CEO of Shared Assessments, a cyber-risk management group, stated that "just the types of test proscribed might indicate a type of illness that you would not want employers or insurance companies to have. Thieves often steal and resell insurance data on the internet…having other information makes the data more valuable and the price higher."[52]

111. Personal Information is a valuable commodity to identity thieves. Compromised Personal Information is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, social security numbers and other Personal Information directly on various dark web sites making the information publicly available.[53]

112. Further, medical databases are particularly high value targets for identity thieves. According to one report, a stolen medical identity has a $50 street value on the black market, whereas a Social Security number sells for only $1.[54]

---

51 *Id.*

52 *Id.*

53 *Here's How Much Your Personal Information Is Selling for on the Dark Web,* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 17, 2019); McFarland et al., *The Hidden Data Economy*, at 3, *available at* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf (last visited June 17, 2019).

54 *Study: Few Aware of Medical Identity Theft Risk*, Claims Journal (June 14, 2012), https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited June 10, 2019).

113. LabCorp is well aware that its own data and the data it shares with AMCA contained a treasure trove of material for hackers as it has been targeted in the past. In July 2018, one month before the Data Breach began, LabCorp was hit with a ransomware attack where attackers locked up files and other data, demanding payment to release them. The attack affected tens of thousands of LabCorp workstations, servers and devices.

114. In a note to employees about the ransomware attack, LabCorp included a prewritten question-and-answer section. One question read: "How certain are we that no data was lost or compromised as a result of this ransomware incident, including patient data?" The answer didn't provide a degree of certainty. It read: "At this time, there is no evidence of theft or misuse of data."

H. LabCorp Has Harmed Plaintiffs And Class Members By Allowing Anyone To Access Their Information

115. LabCorp caused harm to Plaintiffs and Class Members by sharing their Personal Information with AMCA without properly monitoring its business associate, and AMCA failed to prevent attackers from accessing and stealing this information in the Data Breach.

116. Given the sensitive nature of the Personal Information stolen in the Data Breach – including names, mailing addresses, phone numbers, dates of birth, Social Security numbers, information related to Plaintiffs' and Class Members' medical providers and services (such as dates of service, and referring doctor) and other personal information – such as credit and debit card numbers, bank account information, insurance, insurance subscriber identification number – hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future.

117. In fact, many victims of the Data Breach have likely already experienced harms as the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud,

unauthorized lines of credit opened in their names, medical and healthcare fraud, and unauthorized access to their bank accounts. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

118. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest. Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail, extortion, and other negative effects.

119. In a data breach implicating a medical provider or medical information, consumers face the additional risk of their Health Savings Accounts ("HSAs") being compromised. HSAs are often tied to specialized debit cards used to make medical-based payments. However, they can also be used for regular purchases (albeit incurring a severe tax penalty). Such information is an "easy target" for criminal actors.[55]

120. Fraudulent charges have already been linked to Defendant's billing collector's data handling. LabCorp publicly revealed the exposure of patients' Personal Information only after "a

[55] *Id.*

disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges."[56]

121. In addition, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 disclosed that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[57] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high-interest payday loan versus a lower-interest loan.

122. As explained further by the FTC, medical identity theft can have other serious consequences:

> Medical ID thieves may use your identity to get treatment – even surgery – or to bilk insurers by making fake claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits, and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[58]

---

[56] Declaration of Russell H. Fuchs Pursuant to Local Bankruptcy Rule 1007-2 and in Support of "First Day" Motions, *In re Retrieval-Masters Creditors Bureau, Inc.*, No. 19-23185-RDD (Bankr. S.D.N.Y. June 17, 2019), ECF No. 2 at 5-6.

[57] *The Aftermath 2017*, Identity Theft Resource Center, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Aug. 9, 2019).

[58] *Medical ID Theft: Health Information for Older People*, Federal Trade Commission, *available at* https://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people (last visited October 7, 2019).

123. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[59]

124. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their Personal Information;

b. identity theft and fraud resulting from the theft of their Personal Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

---

[59] *See Study: Medical identity theft is costly for victims,* CNET (Mar. 3, 2010), *available at* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited October 11, 2019).

h. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

125. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[60]

126. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[61]

127. Plaintiffs and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that

---

[60] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Aug. 9, 2019).

[61] U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (2007), *available at* http://www.gao.gov/new.items/d07737.pdf

has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[62]

128. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, Defendant would have no reason to tout their data security efforts to their actual and potential customers.

129. Consequently, had consumers known the truth about Defendant's data security practices – that they did not adequately protect and store their Personal Information – they would not have entrusted their Personal Information to LabCorp.

130. Reactions to the Data Breach reflect the severity and breadth of the adverse impact on the American public. Senators Robert Menendez and Cory A. Booker of New Jersey have requested information to LabCorp stating:

> This isn't the first time LabCorp has come under scrutiny due to information security concerns. As recently as June 2018 your company faced a lawsuit charging LabCorp with a HIPAA violation for failing to provide adequate privacy protections at its Providence Hospital computer intake station. In July 2018, just one month before the AMCA breach began, the company's IT network was compromised, again leaving the information of millions of your patients vulnerable. In light of LabCorp's history of information security challenges, the company has both the knowledge and responsibility to heighten information security standards and processes to better protect the patients it serves.[63]

---

[62] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited Aug. 9, 2019).

[63] Letter from U.S. Senators Robert Menendez and Cory A. Booker (June 5, 2019), *available at* https://www.menendez.senate.gov/imo/media/doc/06.05.19%20LabCorp%20Letter.pdf

131. The Attorneys General of Colorado, Connecticut, Illinois, Florida, New York, and Indiana have requested LabCorp provide information about the Data Breach. The request from Indiana's Attorney General included a Civil Investigative Demand.[64]

132. Connecticut Attorney General William Tong, announcing that Illinois and Connecticut's Attorneys General have opened an investigation into the Data Breach, stated:

> The last thing patients should have to worry about is whether their personal information has been compromised by the entities responsible for protecting it. I am committed to ensuring that impacted patients receive timely notification and that the companies involved take precautions to protect consumers' sensitive health and financial information in the future.[65]

133. Other State Attorneys General, including the Attorneys General of Michigan, Minnesota, and North Carolina, have also launched investigations into the Data Breach.[66]

CLASS ACTION ALLEGATIONS
NATIONWIDE CLASS

134. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

---

[64] LabCorp Form 8-K (August 8, 2019), https://www.sec.gov/ix?doc=/Archives/edgar/data/920148/000092014819000076/lh201910-qq2.htm

[65] *Connecticut and Illinois Open Investigation into Quest Diagnostics, LabCorp Data Breach*, The Office of Attorney General William Tong, *available at* https://portal.ct.gov/AG/Press-Releases/2019-Press-Releases/CT-AND-IL-OPEN-INVESTIGATION-INTO-QUEST-AND-LABCORP-DATA-BREACH.

[66] *AMCA Data Breach Tally Passes 20 Million as BioReference Laboratories Added to List of Impacted Entities*, HIPPA Journal, https://www.hipaajournal.com/amca-data-breach-tally-passes-20-million-as-bioreference-laboratories-added-to-list-of-impacted-entities/ (last visited October 9, 2019).

> All natural persons residing in the United States whose Personal Information was compromised in the Data Breach**.**

135. The Nationwide Class asserts claims under North Carolina law against Defendant for violation of the negligence (Count 1), negligence *per se* (Count 2), unjust enrichment (Count 3), declaratory judgment (Count 4), breach of implied contract (Count 5) and the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. §75-1.1, *et seq.* (Count 6) and the North Carolina Identity Theft Protection Act, N.C. Gen. Stat. §75-60, *et seq.* (Count 7) .

STATEWIDE [NAME OF STATE] SUBCLASS

136. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of state-by-state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes (Counts 8 through 29), on behalf of separate statewide subclasses for each State (the "Statewide Subclasses"), defined as follows:

> All natural persons residing in [name of state or territory] whose Personal Information was compromised in the Data Breach.

137. Excluded from the Nationwide Class and each Statewide Subclass are Defendant, any entity in which either Defendant has a controlling interest, and either Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and each Statewide Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

138. **Numerosity: Federal Rule of Civil Procedure 23(a)(1)**. The members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, Defendant has acknowledged that millions of LabCorp customers' Personal

Information has been compromised. Those individuals' names and addresses are available from Defendant's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least thousands of Class Members in each Statewide Subclass, making joinder of all Statewide Subclass members impracticable.

139. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

a. Whether Defendant had a duty to protect Personal Information;

b. Whether Defendant failed to take reasonable and prudent security measures;

c. Whether Defendant knew or should have known of the susceptibility of AMCA's systems to a data breach;

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

e. Whether Defendant's security measures to protect its systems were reasonable in light known legal requirements;

f. Whether Defendant was negligent in failing to adequately monitor and audit the data security systems of its vendors and business associates;

g. Whether Defendant's efforts (or lack thereof) to ensure the security of patients' Personal Information provided to business associates were reasonable in light of known legal requirements;

h. Whether Defendant's conduct constituted unfair or deceptive trade practices;

i. Whether Defendant violated state law when they failed to implement reasonable security procedures and practices;

j. Which security procedures and notification procedures Defendant should be required to implement;

k. Whether Defendant has a contractual obligation to use reasonable security measures;

l. Whether Defendant has complied with any contractual obligation to use reasonable security measures;

m. What security measures, if any, must be implemented by Defendant to comply with its contractual obligations;

n. Whether Defendant violated state consumer protection and state medical information privacy laws in connection with the actions described herein;

o. Whether Defendant failed to notify Plaintiffs and Class Members as soon as practicable and without delay after the data breach was discovered;

p. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of AMCA's systems and/or the loss of the Personal Information of Plaintiffs and Class Members;

q. Whether Plaintiffs and Class Members were injured and suffered damages or other losses because of Defendant's failure to reasonably protect their Personal Information; and,

r. Whether Plaintiffs and Class Members are entitled to damages, declaratory or injunctive relief.

140. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class Members. Plaintiffs' Personal Information was in Defendant's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class Members and Plaintiffs seek relief consistent with the relief of the Class.

141. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

142. **Predominance & Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate

their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

143. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for Defendant or would be dispositive of the interests of members of the proposed Class.

144. **Ascertainability.** The Class and Subclasses are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the class. The Class and Subclasses consist of individuals who received services from LabCorp and whose accounts were placed into collections with AMCA by LabCorp. Class Membership can be determined using LabCorp and AMCA's records in their databases.

145. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

146. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Defendant failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiffs and the Class Members;

c. Whether Defendant failed to adequately monitor and audit the data security systems of its vendors and business associates;

d. Whether adherence to HIPAA regulations, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1

NEGLIGENCE

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

147. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

148. LabCorp required Plaintiffs and Class Members to submit Personal Information to obtain diagnostic and medical services, which LabCorp provided to AMCA for billing purposes. LabCorp collected and stored the Personal Information for commercial gain.

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

150. Defendant had a non-delegable duty to ensure that contractual partners with whom they shared patient information maintained adequate and commercially-reasonable data security practices to ensure the protection of patients' Personal Information.

151. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' Personal Information within its control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

152. Defendant owed a duty of care to Plaintiffs and members of the Class to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the Personal Information.

153. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and the Plaintiffs and Class Members. The special relationship arose because Plaintiffs and Class Members entrusted Defendant with their confidential data as part of the health treatment process. Only Defendant was in a position to ensure that its contractual partners had sufficient safeguards to protect against the harm to Plaintiffs and Class Members that would result from a data breach.

154. Defendant's duty to use reasonable care in protecting Personal Information arose as a result of the common law and the statutes and regulations, as well as its own promises regarding privacy and data security to its patients. This duty exists because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of Plaintiffs and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they

would be harmed in the future if Defendant did not protect Plaintiffs' and Class Members' information from hackers.

155. Defendant's duties also arose under HIPPA regulations, which, as described above, applied to Defendant and establish national standards for the protection of patient information, including protected health information, which required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The duty also arose under HIPAA's Privacy Rule requirement that Defendant obtain satisfactory assurances from its business associate AMCA that AMCA would appropriately safeguard the protected health information it receives or creates on behalf of the Defendant. 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

157. Defendant knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its vendors' and business associates' systems, and the importance of adequate security. LabCorp specifically knew about the risks inherent in collecting and storing Personal Information given its experience with a recent cyber-attack in July

2018 and its acknowledgment that LabCorp's "business associates" are "required to maintain the privacy and confidentiality of [patients'] PHI."

158. Defendant breached its common law, statutory, and other duties – and thus were negligent – by failing to use reasonable measures to protect patients' Personal Information, and by failing to provide timely and adequately detailed notice of the Data Breach.

159. Defendant breached its duties to Plaintiffs and Class Members in numerous ways, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs' and Class Members' Personal Information;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to adequately monitor and audit the data security systems of its vendors and business associates;

d. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

e. Failing to adequately monitor, evaluate, and ensure the security of AMCA's network and systems;

f. Failing to recognize in a timely manner that Plaintiffs' and other Class Members' Personal Information had been compromised; and

g. Failing to timely and adequately disclose that Plaintiffs' and Class Members' Personal Information had been improperly acquired or accessed.

160. Plaintiffs' and Class Members' Personal Information would not have been compromised but for Defendant's wrongful and negligent breach of its duties.

161. Defendant's failure to take proper security measures to protect sensitive Personal Information of Plaintiffs and Class Members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Personal Information of Plaintiffs and Class Members.

162. It was also foreseeable that Defendant's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and other Class Members.

163. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their Personal Information as described in this Complaint.

164. As a direct and proximate cause of Defendant's conduct, Plaintiffs and the Class suffered damages and will suffer damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Personal Information of Plaintiff and Class Members; damages arising from identity theft or fraud; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take years to discover and detect; and loss of the value of their privacy and confidentiality of the stolen confidential data, including health data.

COUNT 2

NEGLIGENCE PER SE
On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

165. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

166. Defendant is an entity covered by HIPAA (45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

167. HIPAA requires Defendant 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). HIPAA also requires Defendant to obtain satisfactory assurances that its business associates would appropriately safeguard the protected health information it receives or creates on behalf of the Defendant. 45 CFR § 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA. AMCA constitutes a "business associate" within the meaning of HIPAA.

168. HIPAA further requires Defendant to disclose the unauthorized access and theft of the Personal Information to Plaintiffs and the Class Members "without unreasonable delay" so that Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information. *See* 45 C.F.R. §§ 164.404, 406, 410.

169. Defendant violated HIPAA by failing to reasonably protect Plaintiffs' and Class Members' Personal Information, as described herein.

170. Defendant's violations of HIPAA constitute negligence per se.

171. Plaintiffs and Class Members are within the class of persons that HIPAA was intended to protect.

172. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

173. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

174. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

175. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as LabCorp, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

176. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

177. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

178. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

179. As a direct and proximate result of Defendant's negligence per se under HIPAA and the FTC Act, Plaintiffs and the Class have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT 3

UNJUST ENRICHMENT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

180. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

181. Plaintiffs and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by Defendant and which was ultimately stolen in the Data Breach.

182. Defendant received a monetary benefit from Plaintiff and Class Members' conferring upon them their Personal Information, which Defendant retain and use for business purposes and profit.

183. Plaintiffs' and the Class Members' Personal Information was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that Personal Information.

184. But for Defendant's commitment to maintain the confidentiality and security of their Personal Information, Plaintiffs and the Class Members would not have provided the information to Defendant.

185. As a result of the wrongful conduct alleged herein, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members. Among other things, Defendant continues to benefit and profit from the use of Plaintiffs' and the Class Members' Personal Information, while its value to Plaintiffs and Class Members has been diminished and its exposure has caused Plaintiffs and Class Members harm.

186. Under the doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits they received, and are still receiving, from Plaintiffs and Class Members.

187. Equity and good conscience require restitution by the Defendant in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including, specifically, the value to Defendant of the Personal Information that was stolen in the Data Breach and the resulting profits Defendant received and are receiving from the use of that information.

COUNT 4

DECLARATORY JUDGMENT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

188. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

189. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the Personal Information it

collected from them. As previously alleged, Defendant owe duties of care to Plaintiff and Class Members that require them to adequately secure Personal Information.

190. Defendant still possesses Personal Information pertaining to Plaintiffs and Class Members.

191. Defendant has made no announcement or notification that they have remedied the vulnerabilities in its practices and policies regarding ensuring the data security of patients' Personal Information.

192. Accordingly, Defendant has not satisfied its implied contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendant's lax approach towards data security has become public, the Personal Information in its possession and in its vendors and business associates' possession is more vulnerable than it was prior to announcement of the Data Breach.

193. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class Members, including the fact that Class Members' Personal Information was available for sale on the dark web.

194. Plaintiffs, therefore, seek a declaration that (a) Defendant's existing data security measures do not comply with its obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Modifying its practices and policies to ensure the business associates to which they provide patients' Personal Information engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing,

including simulated attacks, penetration tests, and audits on its systems on a periodic basis, and ordering vendors and business associates to promptly correct any problems or issues detected by such third-party security auditors;

b. Modifying its practices and policies to ensure the business associates to which they provide patients' Personal Information engage third-party security auditors and internal personnel to run automated security monitoring;

c. Modifying its practices and policies to ensure the business associates to which they provide patients' Personal Information audit, test, and train security personnel regarding any new or modified procedures;

d. Modifying its practices and policies to ensure the business associates to which it provides patients' Personal Information segment Personal Information by, among other things, creating firewalls and access controls so that if one area of a system is compromised, hackers cannot gain access to other portions of the systems;

e. Modifying its practices and policies to ensure only Personal Information necessary for provision of services is provided to business associates;

f. Modifying its practices and policies to ensure Personal Information not necessary for the provision of services is purged, deleted, and destroyed, and to ensure its business associates likewise purge, delete, and destroy such Personal Information;

g. Conducting regular security checks of the business associates to which it provides patients' Personal Information;

h. Routinely and continually conduct internal training and education to inform internal security personnel how to monitor the data security of business associates to whom patients' Personal Information is provided; and

i. Educating its patients about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendant's patients must take to protect themselves.

COUNT 5

BREACH OF IMPLIED CONTRACT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

195. Plaintiffs repeat the allegations set forth in the preceding paragraphs as if fully set forth herein.

196. Plaintiffs and Class Members were required to provide their Personal Information, including names, addresses, Social Security numbers, financial information, and other personal information, to LabCorp in order to complete medical and diagnostic tests.

197. When Plaintiffs and Class Members provided their Personal Information to LabCorp in exchange for services, they entered into implied contracts with LabCorp pursuant to which LabCorp agreed to safeguard and protect such information and to timely and adequately notify them if their data had been breached and compromised.

198. Plaintiffs and the Class Members would not have provided and entrusted their Personal Information to Defendant in the absence of the implied contract to keep the information secure.

199. Plaintiffs and the Class Members fully performed their obligations under the implied contract with Defendant by providing their Personal Information, whereas Defendant did not comply with its obligations to keep the information secure.

200. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs and Class Members' Personal Information, which was compromised as a result of the Data Breach.

201. As a direct and proximate result of Defendant's breach of their implied contacts with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity as to how their Personal Information is used; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (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 the Personal Information in their continued possession; and, (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 Data Breach for the remainder of the lives of Plaintiffs and Class Members.

COUNT 6

NORTH CAROLINA UNFAIR TRADE PRACTICES
On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the North Carolina Subclass

202. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

203. This cause of action is brought under North Carolina's Unfair Trade Practice Act, N.C. Gen. Stat. §75.1.1, *et seq.* (the "NCUTPA").

204. Under the NCUTPA, unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful.

205. At all times material hereto, Defendant committed unfair or deceptive acts or practices in violation of NCUTPA by committing acts or practices that, *inter alia*, offend established public policy, as embodied in North Carolina privacy laws and Section 5 of the FTC Act, and are immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers including, but not limited to, representing that goods or services have characteristics, uses, or benefits that they do not have.

206. Defendant's unfair and deceptive acts or practices possessed the tendency or capacity to mislead, or created the likelihood of deception, of an average, reasonable consumer.

207. At all times material hereto, Defendant's action in committing an unfair or deceptive act or practice was in or affecting commerce.

208. Defendant's unfair or deceptive actions proximately caused injury to Plaintiffs and the Class.

209. Defendant engaged in unfair or deceptive acts willfully, and has refused to take responsibility for them.

210. Under to §75-16 of the NCUTPA, judgment shall be for treble the amount fixed by the verdict. And pursuant to §75-16.1 of the NCUTPA, a reasonable attorney fee should be allowed as part of the court costs.

COUNT 7

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

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the North Carolina Subclass

211. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

212. Defendant is a "business" that owns or licenses computerized data that includes Personal Information as defined by N.C. Gen. Stat. § 75-61(1).

213. Plaintiff and Class members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

214. Defendant is required to accurately notify Plaintiff and Class members if they discover a security breach, or receive notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

215. Plaintiff's and Cllass members' Personal Information includes Personal Information as covered under N.C. Gen. Stat. § 75-61(10).

216. Because Defendant discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons) of AMCA's data systems involving the Personal Information of Plaintiff and North Carolina Subclass members that Defendant provided to AMCA, Defendant had an

obligation to disclose the Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

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

218. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

219. As a direct and proximate result of Defendant's violations of N.C. Gen. Stat. § 75-65, Plaintiff and Class members suffered damages, as described above.

220. Plaintiff and Class members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorney's fees.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 8

CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT, Cal. Civ. Code §§ 56, *et seq.*

221. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

222. California's Confidentiality of Medical Information Act ("CMIA") requires a healthcare provider "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information [to] do so in a manner that preserves the confidentiality of the information contained therein." Cal. Civ. Code § 56.101. "Every provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores,

abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36." *Id.*

223. The CMIA further requires that "[a]n electronic health record system or electronic medical record system . . . [p]rotect and preserve the integrity of electronic medical information." Cal. Civ. Code § 56.101(b)(1)(A).

224. Plaintiff and California Sub-Class members are "patient[s]," "whether or not still living, who received health care services from a provider of health care and to whom medical information pertains" pursuant to § 56.05(k) of the CMIA.

225. Defendant is a "provider of healthcare" pursuant to § 56.05(m) of the CMIA "who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information."

226. Defendant is subject to the requirements and mandates of the CMIA.

227. The Personal Information of Plaintiff and California Subclass members compromised in the Data Breach constitutes "medical information" maintained in electronic form pursuant to § 56.05(j) of the CMIA.

228. Defendant violated § 56.36(b) of the CMIA by negligently maintaining, preserving, storing and releasing the Personal Information of Plaintiff and California Subclass members, and failing to protect and preserve the integrity of the Personal Information of Plaintiff and California Subclass members.

229. Plaintiff and California Subclass members did not authorize Defendant's disclosure and release of their Personal Information that occurred in the Data Breach.

230. As a result of the Data Breach, the Personal Information of Plaintiff and California Subclass members was compromised when it was acquired and accessed by unauthorized parties.

231. Defendant violated the CMIA by negligently (1) failing to implement reasonable administrative, physical and technical safeguards to protect, secure and prevent the unauthorized access to, and acquisition of, Plaintiff's and California Subclass members' Personal Information; (2) failing to implement reasonable data security measures, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiff's and California Subclass members' Personal Information and ensuring its vendors and business associates implemented such measures; (3) failing to use reasonable authentication procedures to track Personal Information in case of a security breach and ensuring its vendors and business associates implemented such measures; and (4) allowing undetected and unauthorized access to servers, networks and systems where Plaintiff's and California Subclass members' Personal Information was kept, all in violation of the CMIA.

232. Defendant's failure to implement adequate data security measures to protect the Personal Information of Plaintiff and California Subclass members was a substantial factor in allowing unauthorized parties to access AMCA's computer systems and acquire the Personal Information of Plaintiff and California Subclass members.

233. As a direct and proximate result of Defendant's violation of the CMIA, Defendant allowed the Personal Information of Plaintiff and California Subclass members to: (a) escape and spread from its normal place of storage through unauthorized disclosure or release; and (b) be accessed and acquired by unauthorized parties in order to, on information and belief, view, mine, exploit, use, and/or profit from their Personal Information, thereby breaching the confidentiality of their Personal Information. Plaintiff and California Subclass members have accordingly sustained and will continue to sustain actual damages as set forth above.

234. Plaintiff and California Subclass members seek actual and statutory damages pursuant to § 56.36(b)(1) of the CMIA.

235. Plaintiff and California Subclass members also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23, Civil Code § 56.35, and California Code of Civil Procedure § 1021.5.

COUNT 9

CALIFORNIA CUSTOMER RECORDS ACT,
Cal. Civ. Code §§ 1798.80, *et seq.*

236. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

237. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

238. Defendant is a business that own, maintain, and license Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass members.

239. Businesses that own or license computerized data that includes Personal Information are required to notify California residents when their Personal Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data

security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

240. Defendant is a business that own or license computerized data that includes Personal Information as defined by Cal. Civ. Code § 1798.82.

241. Plaintiff and California Subclass members' Personal Information includes Personal Information as covered by Cal. Civ. Code § 1798.82.

242. Because Defendant reasonably believed that Plaintiff's and California Subclass members' Personal Information was acquired by unauthorized persons during the Data Breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

243. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Cal. Civ. Code § 1798.82.

244. As a direct and proximate result of Defendant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above.

245. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT 10

CALIFORNIA UNFAIR COMPETITION LAW,
Cal. Bus. & Prof. Code §§ 17200, *et seq.*

246. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

247. Defendant is a "person" as defined by Cal. Bus. & Prof. Code §17201.

248. Defendant violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

249. Defendant's "unfair" acts and practices include:

a. Failing to implement and maintain reasonable security measures to protect Plaintiff and California Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass, whose Personal Information has been compromised.

b. Failing to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, HIPAA, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

c. Failing to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of AMCA's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

250. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, HIPAA, and California common law.

251. Defendant's unlawful, unfair, and deceptive acts and practices include:

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and California's

Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*.;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California 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 California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80*, et seq.*

252. Defendant's representations and omissions were material because it was likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

253. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or

property; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

254. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff and California Subclass members' rights. LabCorp's past data breaches and breaches within the medical industry put it on notice that its security and privacy protections were inadequate.

255. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their Personal Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 11

CALIFORNIA CONSUMER LEGAL REMEDIES ACT, Cal. Civ. Code §§ 1750, *et seq.*

256. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

257. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq*. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

258. Defendant is a "person" as defined by Civil Code §§ 1761(c) and 1770, and have provided "services" as defined by Civil Code §§ 1761(b) and 1770.

259. Civil Code section 1770, subdivision (a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

260. Civil Code section 1770, subdivision (a)(7) prohibits one who is involved in a transaction from "[r]epresenting that goods or services are of a particular standard, quality, or grade . . . if they are of another."

261. Plaintiff and the California Class are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

262. Defendant's acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including, but not limited to, the following:

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 when they were not;

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

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

263. Defendant's representations and omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

264. Had Defendant disclosed to Plaintiff and Class Members that AMCA's data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and Class Members' Personal Information as part of the services it provided without advising Plaintiffs and Class Members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class Members' Personal Information. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

265. As a direct and proximate result of Defendant's violations of California Civil Code § 1770, Plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

266. Plaintiff and the California Subclass have provided notice of their claims for damages to Defendant, in compliance with California Civil Code § 1782(a).

267. Plaintiff and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

COUNT 12

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

268. The Florida Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Florida Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

269. Plaintiff and Florida Subclass members are "consumers" as defined by Fla. Stat. § 501.203.

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

271. Defendant 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:

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

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

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Florida Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Florida Subclass members' Personal Information or ensure its vendors and business associates reasonably or adequately secured such 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 Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Florida's data security statute, F.S.A. § 501.171(2).

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

273. Had Defendant disclosed to Plaintiff and Class Members that AMCA's data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Class Members' Personal Information as part of the services it provided without advising Plaintiffs and Class Members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class Members' Personal Information. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

274. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and practices, Plaintiff 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 losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

275. Plaintiff 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.

CLAIMS ON BEHALF OF THE KANSAS SUBCLASS

COUNT 13

PROTECTION OF CONSUMER INFORMATION
Kan. Stat. Ann. §§ 50-7a02(a), *et seq*.

276. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

277. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by Kan. Stat. Ann. § 50-7a02(a).

278. Plaintiff's and Kansas Subclass members' Personal Information includes Personal Information as covered under Kan. Stat. Ann. § 50-7a02(a).

279. Defendant is required to accurately notify Plaintiffs and Kansas Subclass members if they become aware of a breach of its data security systems that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

280. Because Defendant was aware of a breach of its vendor AMCA's security system involving the Personal Information of Plaintiff and Kansas Subclass members that Defendant provided to AMCA and that was reasonably likely to have caused misuse of Plaintiffs' and Kansas Subclass members' Personal Information, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

281. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Kan. Stat. Ann. § 50-7a02(a).

282. As a direct and proximate result of Defendant's violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Kansas Subclass members suffered damages, as described above.

283. Plaintiff and Kansas Subclass members seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

COUNT 14

KANSAS CONSUMER PROTECTION ACT, K.S.A. §§ 50-623, *et seq.*

284. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

285. K.S.A. §§ 50-623, et seq. is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

286. Plaintiff and Kansas Subclass members are "consumers" as defined by K.S.A. § 50-624(b).

287. The acts and practices described herein are "consumer transactions," as defined by K.S.A. § 50-624(c).

288. Defendant is a "supplier" as defined by K.S.A. § 50-624(l).

289. Defendant advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

290. Defendant engaged in deceptive and unfair acts or practices, including:

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Kansas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Kansas Subclass members' Personal

Information or ensure its vendors and business associates reasonably or adequately secured such 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 Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b.

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

292. Defendant intended to mislead Plaintiff and Kansas Subclass members and induce them to rely on its misrepresentations and omissions.

293. Had Defendant disclosed to Plaintiff and Class Members that AMCA's data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Class Members' Personal Information as part of the services it provided without advising Plaintiffs and Class Members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class Members' Personal Information. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

294. Defendant also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

a. Knowingly taking advantage of the inability of Plaintiff and the Kansas Subclass to reasonably protect their interests, due to their lack of knowledge. K.S.A. § 50-627(b)(1); and

b. Requiring Plaintiff and the Kansas Subclass to enter into a consumer transaction on terms that Defendant knew were substantially one-sided in favor of Defendant, K.S.A. § 50-627(b)(5).

295. Plaintiff and the Kansas Subclass had unequal bargaining power with respect to their ability to control the security and confidentiality of their Personal Information in Defendant's possession.

296. The above unfair, deceptive, and unconscionable practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

297. Defendant acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act, and recklessly disregarded Plaintiff and Kansas Subclass members' rights. LabCorp's past data breaches and breaches within the medical industry put them on notice that its security and privacy protections were inadequate.

298. As a direct and proximate result of Defendant's unfair, deceptive, and unconscionable trade practices, Plaintiff and Kansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from fraud and identity theft; costs for credit monitoring and

identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

299. Plaintiff and Kansas Subclass members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; restitution; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KENTUCKY SUBCLASS

COUNT 15

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

300. The Kentucky Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein. .

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

302. Plaintiff's and Kentucky Subclass members' Personal Information includes Personal Information as covered under Ky. Rev. Stat. Ann. § 365.732(2).

303. Defendant is required to accurately notify Plaintiff and Kentucky Subclass members if they become aware of a breach of its data security systems that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

304. Because Defendant was aware of a breach of its vendor AMCA's security system involving the Personal Information of Plaintiff and Kentucky Subclass members that Defendant provided to AMCA that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass members' Personal Information, Defendant had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

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

306. As a direct and proximate result of Defendant's violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiff and Kentucky Subclass members suffered damages, as described above.

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

COUNT 16

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

308. The Kentucky Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

309. Defendant is a "person" as defined by Ky. Rev. Stat. § 367.110(1).

310. Defendant 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).

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

a. 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 Data 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 Data Breach;

c. 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, and HIPAA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Kentucky Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

e. Misrepresenting that it would 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, and HIPAA;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Kentucky Subclass members' Personal

Information or ensure its vendors and business associates reasonably or adequately secured such 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 Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

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

313. Defendant intended to mislead Plaintiff and Kentucky Subclass members and induce them to rely on its misrepresentations and omissions.

314. Plaintiff 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 Defendant's unlawful acts and practices.

315. The above unlawful acts and practices by Defendant 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.

316. Defendant acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiff and Kentucky Subclass members' rights. LabCorp's past data breaches and breaches within the medical industry put them on notice that its security and privacy protections were inadequate.

317. As a direct and proximate result of Defendant's unlawful acts and practices, Plaintiff and Kentucky Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

318. Plaintiff and Kentucky Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution or other equitable relief, injunctive relief, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MARYLAND SUBCLASS

COUNT 17

MARYLAND CONSUMER PROTECTION ACT, Md. Code Ann. Com. Law § 13-101, *et seq.*

319. The Maryland Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maryland Subclass, repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

320. Defendant is a person as defined by Md. Code, Com Law § 13-101(h).

321. Defendant's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Code, Com. Law § 13-101(i) and § 13-303.

322. Maryland Subclass members are "consumers" as defined by Md. Code, Com. Law § 13-101(c).

323. Defendant advertises, offers, or sell "consumer goods" or "consumer services" as defined by Md. Code, Com. Law § 13-101(d).

324. Defendant advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

325. Defendant engaged in unfair and deceptive trade practices, in violation of Md. Code, Com. Law § 13-301, including:

a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers, Md. Code, Com. Law § 13-301(1);

b. Representing that consumer goods or services have a characteristic that they do not have, Md. Code, Com. Law § 13-301(2)(i);;

c. Representing that consumer goods or services are of a particular standard, quality, or grade that they are not, Md. Code, Com. Law § 13-301(2)(iv);

d. Failing to state a material fact where the failure deceives or tends to deceive, Md. Code, Com. Law § 13-301(3);

e. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered, Md. Code, Com. Law § 13-301(5);

f. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental, Md. Code, Com. Law § 13-301(9).

326. Defendant engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services in violation of Md. Code, Com Law § 13-303, including:

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maryland Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Code, Com. Law § 14-3503, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Maryland 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 Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Code, Com. Law § 14-3503;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maryland 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 Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the Maryland Personal Information Protection Act, Md. Code, Com. Law § 14-3503.

327. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information. Defendant's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

328. Defendant intended to mislead Plaintiff and Maryland Subclass members and induce them to rely on its misrepresentations and omissions.

329. Had Defendant disclosed to Plaintiffs and Class Members that its vendors' data systems were not secure and, thus, vulnerable to attack, Defendant 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, Defendant received, maintained, and compiled Plaintiffs' and Maryland Subclass members' Personal Information as part of the services Defendant provided without advising Plaintiffs and Maryland Subclass members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Subclass members' Personal Information. Accordingly, Plaintiff and the Maryland Subclass members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

330. Defendant acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiff and Maryland Subclass members' rights. LabCorp's past data breaches and breaches within the healthcare industry put it on notice that its security and privacy protections were inadequate.

331. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Maryland Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

332. Plaintiff and Maryland Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, disgorgement, injunctive relief, and attorneys' fees and costs.

COUNT 18

MARYLAND PERSONAL INFORMATION PROTECTION ACT, Md. Comm. Code §§ 14-3501, *et seq.*

333. The Maryland Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maryland Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein. .

334. Under Md. Comm. Code § 14-3503(a), "[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security

procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations."

335. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

336. Plaintiff and Maryland Subclass members are "individuals" and "customers" as defined and covered by Md. Comm. Code §§ 14-3502(a) and 14-3503.

337. Plaintiff's and Subclass members' Personal Information includes Personal Information as covered under Md. Comm. Code § 14-3501(d).

338. Defendant did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of Md. Comm. Code § 14-3503.

339. The Data Breach was a "breach of the security of a system" as defined by Md. Comm. Code § 14-3504(1).

340. Under Md. Comm. Code § 14-3504(b)(1), "[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach."

341. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), "[i]f, after the investigation is concluded, the business determines that misuse of the individual's Personal Information has occurred or is reasonably likely to occur as a result of a breach of the security system, the business shall notify the individual of the breach" and that notification "shall be given

as soon as reasonably practical after the business discovers or is notified of the breach of a security system."

342. Because Defendant discovered a security breach and had notice of a security breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

343. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

344. As a direct and proximate result of Defendant violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiff and Maryland Subclass members suffered damages, as described above.

345. Pursuant to Md. Comm. Code § 14-3508, Defendant's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act, 13 Md. Comm. Code §§ 13-101 et seq. and subject to the enforcement and penalty provisions contained within the Maryland Consumer Protection Act.

346. Plaintiff and Maryland Subclass members seek relief under Md. Comm. Code §13-408, including actual damages and attorney's fees.

CLAIMS ON BEHALF OF THE MASSACHUSETTS SUBCLASS

COUNT 19

MASSACHUSETTS CONSUMER PROTECTION ACT, Mass. Gen. Laws Ann. Ch. 93A, §§ 1, *et seq.*

347. The Massachusetts Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Massachusetts Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

348. Defendant, Plaintiff, and Massachusetts Subclass members are "persons" as meant by Mass. Gen. Laws. Ann. ch. 93A, § 1(a).

349. Defendant operates in "trade or commerce" as meant by Mass. Gen. Laws Ann. ch. 93A, § 1(b).

350. Defendant advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. ch. 93A, § 1(b).

351. Plaintiff sent a demand for relief on behalf of the Massachusetts Subclass pursuant to Mass. Gen. Laws Ann. Ch. 93A § 9(3) on November 14, 2019.

352. Defendant engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. ch. 93A, § 2(a), including:

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Massachusetts Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Massachusetts Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Massachusetts Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Massachusetts Subclass members' Personal Information or ensure its vendors and business associates reasonably or adequately secured such 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 Massachusetts Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

353. Defendant's acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that Defendant solely held the true facts about its inadequate security for Personal Information, which Plaintiff and the Massachusetts Subclass members could not have independently discovered.

354. Consumers could not have reasonably avoided injury because Defendant's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Defendant created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

355. Defendant's inadequate data security had no countervailing benefit to consumers or to competition.

356. Defendant intended to mislead Plaintiff and Massachusetts Subclass members and induce them to rely on its misrepresentations and omissions. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

357. Defendant acted intentionally, knowingly, and maliciously to violate Massachusetts's Consumer Protection Act, and recklessly disregarded Plaintiff and Massachusetts Subclass members' rights. LabCorp's past data breaches and breaches within the medical industry put them on notice that its security and privacy protections were inadequate.

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

359. Plaintiff and Massachusetts Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, restitution; injunctive or other equitable relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS

COUNT 20

NEW JERSEY CONSUMER FRAUD ACT, N.J.S.A. § 56:8-1, *et. seq.*

360. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

361. The New Jersey Consumer Fraud Act (the "NJCFA"), N.J.S.A. § 56:8-1, et seq., prohibits the act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression or omission, in connection with the sale or advertisement of any merchandise. The

NJCFA applies whether or not any person has in fact been misled, deceived or damaged thereby. N.J.S.A.§ 56:8-2.

362. Plaintiffs, Defendant, and Class Members are "persons" within the meaning of N.J.S.A. § 56:8-1(d).

363. Defendant sells "merchandise," as defined by N.J.S.A. § 56:8-1, by offering health benefits services to the public.

364. Defendant, operating in New Jersey, engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of health benefits services in violation of N.J.S.A. § 56:8-2, including but not limited to the following:

a. Misrepresenting material facts, pertaining to the sale of health benefits services, to the Plaintiffs and Class Members by representing that it would maintain adequate data security practices and procedures to safeguard Plaintiffs' and Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts, pertaining to the sale of health benefits services, to the Plaintiffs and Class Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs' and Class Members' Personal Information;

c. Knowingly omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class Members' Personal Information with the intent that Plaintiffs and Class Members rely on the omission, suppression, and concealment;

d. Engaging in unconscionable and deceptive acts and practices with respect to the sale of health benefit services by failing to adequately monitor and audit the data security systems of its vendors and business associates and failing to maintain the privacy and security of Plaintiffs and Class Members in violation of duties imposed by and public policies reflected in the FTC Act and HIPAA;

e. Engaging in unconscionable and deceptive acts and practices by failing to disclose the Data Breach to Plaintiffs and Class Members in a timely and accurate manner in violation of N.J.S.A. § 56:8-163;

f. Advertising LabCorp's medical treatments with the intent not to sell it as advertise – *i.e.* with worse data security than advertised; and

g. Representing on its website that it is "committed to the protection of [the patient's] PHI" when, in fact, LabCorp failed to safeguard customers' information by providing it to AMCA who had deficient data security protection.

365. The above unlawful and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

366. Defendant knew or should have known that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' Personal Information and that the risk of a data breach was highly likely. Defendant's actions in engaging in the above-listed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

367. Plaintiffs and Class Members reasonably expected that Defendant would protect their Personal Information and reasonably expected that Defendant would provide truthful statements on its website and privacy policies, and that it would be safe to provide LabCorp with their information. These representations and affirmations of fact made by Defendant, and the facts they concealed or failed to disclose, are material facts that were likely to deceive reasonable consumers, and that reasonable consumers would, and did, rely upon in deciding whether or not to provide their information to LabCorp. Defendant, moreover, intended for consumers, including Plaintiffs and Class Members, to rely on these material facts.

368. As a direct and proximate result of Defendant's unconscionable and deceptive acts and practices, Plaintiffs and Class Members suffered an ascertainable loss in moneys or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information.

369. Plaintiffs and Class Members seek relief under N.J.S.A. § 56:8-19, including but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

COUNT 21

NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT, N.J.S.A. §§ 56:8-163, *et seq.*

370. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

371. Defendant is a business that conducts business in New Jersey under N.J.S.A. § 56:8-163(a).

372. Plaintiff's and New Jersey Subclass members' Personal Information includes Personal Information covered under N.J.S.A. §§ 56:8-163*, et seq*.

373. Under N.J.S.A. § 56:8-163(a), "[a]ny business that conducts business in New Jersey. . . shall disclose any breach of security of [] computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person."

374. Because Defendant discovered a breach of AMCA's security system involving the Personal Information of Plaintiff and New Jersey Subclass members that Defendant provided to AMCA in which such Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated under N.J.S.A. §§ 56:8-163, *et seq*.

375. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated N.J.S.A. § 56:8-163(a).

376. As a direct and proximate result of Defendant's violations of N.J.S.A. § 56:8-163(a), Plaintiff and New Jersey Subclass members suffered the damages described above.

377. Plaintiff and New Jersey Subclass members seek relief under N.J.S.A. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT 22

NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law §§ 349, *et seq.*

378. The New York Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

379. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

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

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

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New York Subclass members' Personal Information, including by

implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

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

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New York Subclass members' Personal Information or ensure its vendors and business associates reasonably or adequately secured such 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 Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

380. Plaintiff and members of the New York Subclass were deceived in New York. They also transacted with Defendant in New York by utilizing Defendant's services in New York.

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

382. Defendant acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass members' rights. LabCorp's past data breaches and breaches within the medical industry put them on notice that its security and privacy protections were inadequate.

383. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

384. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of New Yorkers affected by the Data Breach.

385. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

386. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

CLAIMS ON BEHALF OF THE OHIO SUBCLASS

COUNT 23

OHIO CONSUMER SALES PRACTICES ACT, Ohio Rev. Code §§ 1345.01, *et seq*.

387. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

388. Plaintiff and Ohio Subclass members are "persons," as defined by Ohio Rev. Code § 1345.01(B).

389. Defendant was a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

390. Defendant advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

391. Defendant engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §§ 1345.02, including:

a. Representing that its goods, services, and intangibles had performance characteristics, uses, and benefits that they did not have, in violation of Ohio Rev. Code § 1345.02(B)(1); and

b. Representing that its goods, services, and intangibles were of a particular standard or quality when they were not, in violation of Ohio Rev. Code § 1345(B)(2).

392. Defendant engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code Ann. § 1345.03, including:

a. Knowingly taking advantage of the inability of Plaintiff and the Ohio Subclass to reasonably protect their interest because of their ignorance of the issues discussed herein (Ohio Rev. Code Ann. § 1345.03(B)(1)); and

b. Requiring Plaintiff and the Ohio Subclass to enter into a consumer transaction on terms that Defendant knew were substantially one-sided in favor of Defendant (Ohio Rev. Code Ann. § 1345.03(B)(5)).

393. Defendant's unfair, deceptive, and unconscionable acts and practices include:

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Ohio Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

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

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Ohio Subclass members' Personal Information or ensure its vendors and business associates reasonably or adequately secured such 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 Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

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

395. Defendant intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

396. Defendant acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights. LabCorp's past data breaches and breaches within the medical industry put them on notice that its security and privacy protections were inadequate.

397. Defendant's unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the many Ohioans affected by the Data Breach.

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

399. Plaintiff and the Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including declaratory and injunctive relief, the greater of actual and treble damages or statutory damages, attorneys' fees and costs, and any other appropriate relief.

COUNT 24

OHIO DECEPTIVE TRADE PRACTICES ACT, Ohio Rev. Code §§ 4165.01, *et seq.*

400. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

401. Defendant, Plaintiff, and Ohio Subclass members are each a "person," as defined by Ohio Rev. Code § 4165.01(D).

402. Defendant advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

403. Defendant engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including:

a. Representing that its goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code § 4165.02(A)(7);

b. Representing that its goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code § 4165.02(A)(9); and

c. Advertising its goods and services with intent not to sell them as advertise, in violation of Ohio Rev. Code § 4165.02(A)(11).

404. Defendant's deceptive trade practices include:

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Ohio Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

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

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Ohio Subclass members' Personal Information or ensure its vendors and business associates reasonably or adequately secured such 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 Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

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

406. Defendant intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

407. Defendant acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights. LabCorp's past data breaches and breaches within the medical industry put them on notice that its security and privacy protections were inadequate.

408. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

409. Plaintiff and Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, restitution, attorneys' fees, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE OKLAHOMA SUBCLASS

COUNT 25

OKLAHOMA CONSUMER PROTECTION ACT, Okla. Stat. Tit. 15, §§ 751, *et seq.*

410. The Oklahoma Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oklahoma Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

411. Defendant is a "person," as meant by Okla. Stat. tit. 15, § 752(1).

412. Defendant's advertisements, offers of sales, sales, and distribution of goods, services, and other things of value constituted "consumer transactions" as meant by Okla. Stat. tit. 15, § 752(2).

413. Defendant, in the course of its business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, § 753, including:

a. Making false representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions, in violation of Okla. Stat. tit. 15, § 753(5);

b. Representing, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular standard when they were of another, in violation of Okla. Stat. tit 15, § 753(7);

c. Advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised, in violation of Okla. Stat. tit 15, § 753 (8);

d. Committing unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by section 752(14), in violation of Okla. Stat. tit. 15, § 753(20); and

e. Committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by section 752(13), in violation of Okla. Stat. tit. 15, § 753(20).

414. Defendant's unlawful practices include:

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Oklahoma Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members'

Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Oklahoma Subclass members' Personal Information or ensure its vendors and business associates reasonably or adequately secured such 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 Oklahoma Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

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

416. Defendant intended to mislead Plaintiff and Oklahoma Subclass members and induce them to rely on its misrepresentations and omissions.

417. Had Defendant disclosed to Plaintiff and Class Members that AMCA's data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Class Members' Personal Information as part of the services it provided without advising Plaintiffs and Class Members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class Members' Personal Information. Accordingly, Plaintiff and Class Members acted reasonably in

relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

418. The above unlawful practices and acts by Defendant were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial injury to Plaintiff and Oklahoma Subclass members.

419. Defendant acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiff and Oklahoma Subclass members' rights. LabCorp's past data breaches and breaches within the medical industry put them on notice that its security and privacy protections were inadequate.

420. As a direct and proximate result of Defendant's unlawful practices, Plaintiff and Oklahoma Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

421. Plaintiff and Oklahoma Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS

COUNT 26

PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq.*

422. The Pennsylvania Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

423. Defendant is a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

424. Plaintiff and Pennsylvania Subclass Members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

425. Defendant engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including:

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

426. Defendant's unfair or deceptive acts and practices include:

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Pennsylvania Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

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

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Pennsylvania Subclass Members' Personal Information or ensure its vendors and business associates reasonably or adequately secured such 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 Pennsylvania Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

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

428. Defendant intended to mislead Plaintiff and Pennsylvania Subclass Members and induce them to rely on their misrepresentations and omissions.

429. Had Defendant disclosed to Plaintiffs and Pennsylvania Subclass Members that AMCA's data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and Pennsylvania Subclass Members' Personal Information as part of the services they provided without advising Plaintiffs and Pennsylvania Subclass Members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Pennsylvania Subclass Members' Personal Information. Accordingly, Plaintiff and Pennsylvania Subclass Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

430. Defendant acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass Members' rights.

431. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and Pennsylvania Subclass Members' reliance on them, Plaintiff and Pennsylvania Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

432. Plaintiff and Pennsylvania Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, restitution, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS

COUNT 27

TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT, Tenn. Code Ann. §§ 47-18-2107, *et seq*.

433. The Tennessee Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

434. Defendant is a business that owns or licenses computerized data that includes Personal Information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

435. Plaintiff's and Tennessee Subclass members' Personal Information includes Personal Information as covered under Tenn. Code Ann. § 47-18- 2107(a)(3)(A).

436. Defendant is required to accurately notify Plaintiff and Tennessee Subclass members following discovery or notification of a breach of its data security system in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

437. Because Defendant discovered a breach of AMCA's security system involving the Personal Information of Plaintiff and Tennessee Subclass members that Defendant provided to AMCA in which unencrypted Personal Information was, or is reasonably believed to have been,

acquired by an unauthorized person, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

438. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Tenn. Code Ann. § 47-18-2107(b).

439. As a direct and proximate result of Defendant's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass members suffered damages, as described above.

440. Plaintiff and Tennessee Subclass members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages, injunctive relief, and treble damages.

CLAIMS ON BEHALF OF THE WISCONSIN SUBCLASS

COUNT 28

NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION, Wis. Stat. §§ 134.98(2), *et seq.*

441. The Wisconsin Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

442. Defendant is a business that maintains or licenses Personal Information as defined by Wis. Stat. § 134.98(2).

443. Plaintiff's and Wisconsin Subclass members' Personal Information includes Personal Information as covered under Wis. Stat. § 134.98(1)(b).

444. Defendant is required to accurately notify Plaintiff and Wisconsin Subclass members if they know that Personal Information in its possession has been acquired by a person

whom they have not authorized to acquire the Personal Information within a reasonable time under Wis. Stat. §§ 134.98(2)-(3)(a).

445. Because Defendant knew that Personal Information in its possession had been acquired by a person whom it has not authorized to acquire the Personal Information, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Wis. Stat. § 134.98(2).

446. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Wis. Stat. § 134.98(2).

447. As a direct and proximate result of Defendant's violations of Wis. Stat. § 134.98(3)(a), Plaintiff and Wisconsin Subclass members suffered damages, as described above.

448. Plaintiff and Wisconsin Subclass members seek relief under Wis. Stat. § 134.98, including actual damages and injunctive relief.

COUNT 29

WISCONSIN DECEPTIVE TRADE PRACTICES ACT, Wis. Stat. § 100.18

449. The Wisconsin Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

450. Defendant is a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

451. Plaintiff and Wisconsin Subclass members are members of "the public," as defined by Wis. Stat. § 100.18(1).

452. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Defendant to members of the public for sale, use, or distribution, Defendant made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

453. Defendant also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

454. Defendant's deceptive acts, practices, plans, and schemes include:

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

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

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Wisconsin Subclass members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

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

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Wisconsin Subclass members' Personal Information or ensure its vendors and business associates reasonably or adequately secured such 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 Wisconsin Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA.

455. Defendant intended to mislead Plaintiff and Wisconsin Subclass members and induce them to rely on its misrepresentations and omissions.

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

457. Defendant had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the Personal Information in its possession. This duty

arose because Plaintiff and the Wisconsin Subclass members reposed a trust and confidence in Defendant when they provided their Personal Information to Defendant in exchange for Defendant's services. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Wisconsin Subclass—and Defendant, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendant. Defendant's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems and that of its vendors and business associates;

b. Active concealment of the state of its security and that of its vendors and business associates; and/or

c. Incomplete representations about the security and integrity of its computer and data systems and that of its vendors and business associates, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Wisconsin Subclass that contradicted these representations.

458. Defendant's failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

459. Defendant acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Wisconsin Subclass members' rights. LabCorp's past data breaches and breaches within the medical industry put them on notice that its security and privacy protections were inadequate.

460. As a direct and proximate result of Defendant's deceptive acts or practices, Plaintiff and Wisconsin Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from

fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

461. Defendant had an ongoing duty to all Defendant's customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

462. Plaintiff and Wisconsin Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

REQUESTS FOR RELIEF

Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Co-Lead and Co-Liaison Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Plaintiffs and Class and Subclass members compensatory, consequential, and general damages in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of its unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That Plaintiffs be granted the declaratory relief sought herein;

7. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

8. That the Court award pre- and post-judgment interest at the maximum legal rate; and

9. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.
Interim Lead Counsel for Plaintiffs

By: /s/ James E. Cecchi
JAMES E. CECCHI

Dated: November 15, 2019

Linda P. Nussbaum
Bart D. Cohen
NUSSBAUM LAW GROUP, P.C.
1211 Avenue of the Americas, 40th Floor
New York, New York 10036
(917) 38-9101

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

Tina Wolfson
Brad King
Theodore W. Maya
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, California
(310) 474-9111

Jean S. Martin
John A. Yanchunis
MORGAN & MORGAN
76 South Laura Street, Suite 1100
Jacksonville, Florida 32202
(904) 398-2722

LabCorp Track Co-Lead Counsel

Marc L. Godino
Lionel Z. Glancy
Danielle L. Manning
GLANCY PRONGAY & MURRAY LLP
1925 Century Park East, Suite 2100
Los Angeles, California
(310) 201-9150

LabCorp Track Steering Committee