Exhibit A

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) **FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT: LABCORP**

TABLE OF CONTENTS

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

2. 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 unprotected systems, the threat actor exfiltrated the sensitive personal, financial, and medical information (including physician names, tests ordered, and diagnosis codes that represent conditions and diseases),[1] of millions of LabCorp patients, which was subsequently made available on the illegal marketplace known as the "dark web."[2]

3. Defendant has a duty to safeguard and protect customer information entrusted to them and 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

[1] *See* AMCAPROD00698816 (Patient Collection Services Agreement between LabCorp and AMCA dated Dec. 20, 2018); AMCAPROD00256326 (July 21, 2016 copy of LabCorp EREQ for patient, containing patient's name, DOB, last four digits of SSN, address, and lists all tests ordered and ordering physician).

[2] 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), CNBC, https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.

implemented and maintained adequate data security measures and protocols in order to secure and protect LabCorp customers' data.

4. Plaintiffs and Class Members entrusted Defendant with, and allowed Defendant to gather, highly sensitive information relating to their health and other matters as part of their seek treatment. They did so in confidence, and they had the legitimate expectation that Defendant will respect their privacy and act appropriately.

5. Trust and confidence are key components of Plaintiffs' and Class Members' relationship with Defendant. Without it, Plaintiffs and Class Members would not have provided Defendant with, or allowed Defendant to collect, their most sensitive information in the first place. To be sure, Plaintiffs and Class Members relied upon Defendant to do as they are required by law and implement safeguards in order to ensure their customers' highly sensitive information is stored and at all times transmitted securely and protected from unauthorized access.

6. Plaintiffs bring this class action because Defendant collected and 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 ("SSNs"), 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 debit card numbers, bank account information, insurance, and insurance subscriber identification numbers (all collectively referred to as "Personal Information").

7. 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, many Class Members' identities have already been stolen.

8. Defendant's intentional, willful, reckless, unfair, 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 – harmed Plaintiffs and Class Members uniformly. As discussed herein, fraudulent activities have already been linked to Defendant's unfair and deceptive 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 likewise 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.

9. Defendant has also been unfairly and unjustly enriched as a result of their improper conduct, such that it would be inequitable for them to retain the benefits conferred upon them by Plaintiffs and the other Class Members. Plaintiffs never would have engaged LabCorp to perform medical services and entrusted LabCorp with their Personal Information, had they known that LabCorp would permit unauthorized access to their Personal Information by LabCorp's complete and utter disregard for security safeguards and protocols. Plaintiffs would have used another provider.

JURISDICTION AND VENUE

10. 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.

11. 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.

12. 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.

13. 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

14. 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.

15. Each and every Plaintiff has suffered a concrete and particularized injury as a result of Defendant's known deficient security and failure to protect their Personal Information, as well as their concealment of same, that allowed unauthorized access to their Personal Information.

16. Had Defendant disclosed that they disregarded their duty to safeguard and protect Plaintiffs' Personal Information from unauthorized access, Plaintiffs would have taken them into account in making her healthcare decisions. In particular, had Plaintiffs known about the deficiencies in Defendant's securing, safeguarding, and otherwise protecting Plaintiffs' Personal Information, they would not have engaged Defendant's services or provided their Personal Information to Defendant. Plaintiff would have engaged a competing provider, which would have protected Plaintiffs' Personal Information.

ARKANSAS

17. 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, both at a LabCorp lab facility and through a doctor's office where samples were sent to LabCorp for testing. On information and belief, LabCorp provided Plaintiff Palmer's Personal Information to AMCA as part of its bill collections practice. Ms. Palmer reviewed LabCorp's privacy policies at the time she received the laboratory services. 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. More recently Ms. Palmer has experienced several attempts to open a credit card account in her name that she did not open or authorize. A fraudulent credit card was opened at a Meijer store,

which was issued through a major bank using her name and address. The store tracked the person down to someone in Michigan or Milwaukee, Wisconsin. Fraudulent charges were made on the account and the account is now in default. Ms. Palmer informed them that she does not reside in Michigan or Wisconsin and there is no Meijer store anywhere near her. Ms. Palmer hired a law firm to dispute the charges and monitor any fraudulent activity. The law firm discovered several other attempts to open accounts in her name and discovered there had been other fraudulent credit pulls. The fraudulent account appeared on her credit report. She has had many credit inquiries on her credit reports that were not hers and is working with the law firm to get them removed from her credit. At the beginning of the COVID-19 pandemic, someone also made a fraudulent purchase on Ms. Palmer's bank debit card. The bank refunded the charge to her and issued a new card to her. 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 and obtaining credit monitoring services through Norton. She has received many notifications from Norton that her information has been exposed in a data breach and frequent instructions and prompts to change her passwords. To date, in addition to hiring a law firm, 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. Ms. Palmer values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Palmer's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

CALIFORNIA

18. 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 at a LabCorp lab facility and, on information and belief, LabCorp provided Plaintiff Lassiter's Personal Information to AMCA as part of its bill collections practice. Ms. Lassiter reviewed LabCorp's privacy policies at the time she received the laboratory services. 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 and obtaining fraud monitoring from Norton. She has been informed by the Norton service that her confidential information, including her email, birth date, address and social security number, were on the dark web. 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. Ms. Lassiter values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Lassiter's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

19. 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 through a medical clinic where samples were sent to LabCorp for testing. On information and belief, LabCorp provided Plaintiff Nazemnikov's Personal Information to AMCA as part of

its bill collections practice. If the clinic gave Mr. Nazemnikov the LabCorp privacy policies, he would have reviewed them, but he does not recall if he was given that specific paperwork. 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. Mr. Nazemnikov recalls that at some point after June 2019, someone tried to charge his bank account for a couple thousand dollars of recording equipment from a location in Sweden. The bank shut down the transaction and the fraudulent charges did not successfully go through. He was required to get a new debit card in August 2019. The fraud claim number for that incident was 1808310008443. In addition, Mr. Nazemnikov made another fraud claim with his bank in August of 2018 for a fraudulent charge on his debit card of around $437.00. The fraud claim number for that incident was 10831184586. 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. Mr. Nazemnikov values his privacy. Had he been informed that LabCorp was going to share his personal information with a debt collection agency that had insufficient data security measures, he would never have continued to use the LabCorp services. Plaintiff Nazemnikov's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

FLORIDA

20. 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, both at a LabCorp lab facility and through a doctor's office where samples were sent to LabCorp for testing. On

information and belief, LabCorp provided Plaintiff Buhr's Personal Information to AMCA as part of its bill collections practice. Ms. Buhr reviewed LabCorp's privacy policies at the time she received the laboratory services. On or about July 12, 2019, Plaintiff Buhr received a data breach notification letter from LabCorp. In 2021, there were three attempts to open fraudulent credit cards and store cards using Ms. Buhr's name and information – one credit card and two department store accounts. Her Experian credit report account was also hacked. She had to freeze all of her credit bureau accounts. She had to close her debit card in 2021 after someone tried to charge Uber fees that she did not incur or authorize. The bank was able to block the transaction before it went through. In March 2022, Ms. Buhr received a letter from Wells Fargo advising her that her application for an account was denied, however, Ms. Buhr did not apply for an account with Wells Fargo. 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. Ms. Buhr values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Buhr's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

21. 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 through having bloodwork performed at a local hospital in Calhoun County, Florida and sample sent to LabCorp for testing. On information and belief, LabCorp provided Plaintiff Laufenberg's Personal

Information to AMCA as part of its bill collections practice. Ms. Laufenberg believes she briefly reviewed LabCorp's privacy policies when she initially received the first laboratory services. 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 around the same time as the AMCA/LabCorp data breach. Someone attempted to charge a small amount on her debit card and the bank reversed the charge, closed her debit card account and issued her a new 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. She has used free services like Credit Karma, because she cannot afford to pay for expensive credit monitoring services. She has received notifications from some of the free credit monitoring services that her name and other information have been sold for a certain number of times. 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. Ms. Laufenberg values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Laufenberg's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

GEORGIA

22. 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 at a LabCorp lab facility and, on information and belief, LabCorp provided Plaintiff Haley's Personal Information to AMCA as part of its bill collections practice. Ms. Haley reviewed LabCorp's privacy policies

at the time she received the laboratory services. On or about July 12, 2019, Plaintiff Haley received a data breach notification letter from LabCorp. Ms. Haley has received "hard hits" on her credit report that she did not cause. She uses the free service Credit Karma to monitor her credit reports. There was a credit inquiry for a home loan incurred at some point in 2021 that was not a result of any action taken by Ms. Haley. 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. Ms. Haley values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Haley's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

23. 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 through a doctor's office where samples were sent to LabCorp for testing. 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. In 2020, someone tried to open an off-brand credit card in his name which he did not open or authorize. Mr. Nelson-Carter has a fraud alert set up on his credit report, so he was notified and the attempt was not successful. Mr. Nelson-Carter had to close his bank account in 2020, following fraudulent activity from

Kroger on the account. He was eventually reimbursed for the overdraft fees that resulted. He has received notices of additional credit inquiries and credit pulls that he did not cause or authorize, but none were successful. Mr. Nelson-Carter has been informed by Lookout Mobile and Credit Karma that his confidential information, including his email, phone number and passwords, was on the dark web. 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. Mr. Nelson-Carter values his privacy. Had he been informed that LabCorp was going to share his personal information with a debt collection agency that had insufficient data security measures, he would never have continued to use the LabCorp services. Plaintiff Nelson-Carter's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

24. 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 at a LabCorp lab facility and, on information and belief, LabCorp provided Plaintiff Scott's Personal Information to AMCA as part of its bill collections practice. Ms. Scott reviewed LabCorp's privacy policies at the time she received the laboratory services. On or about July 20, 2019, Plaintiff Scott received a data breach notification letter from LabCorp. In October 2019, Ms. Scott's credit card was compromised. She received a text message from the credit card company asking her if she authorized the transaction. After denying the charge was hers, Ms. Scott received a new credit card from the credit card company with a new account number. The unauthorized charge on the

credit card was discovered by the credit card company before it went through the account. On January 14, 2022, Ms. Scott received an alert from a different credit card company asking if she authorized a charge to the Nebraska Children's Home Society. Ms. Scott replied that she had not authorized and disputed the charge. Ms. Scott then received a new card from the credit card company with a new account number. Ms. Scott has been informed by credit monitoring services on a number of occasions that her passwords for certain accounts were found on the "dark web." The service then recommends that she change her passwords, and she does so each time she receives those notices. Ms. Scott's children have had fraud occur on their bank accounts, where her name was on their bank accounts at the time. She has since removed her name from their bank accounts. 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. Ms. Scott values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Scott's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

KANSAS

25. 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, both at a LabCorp lab facility and through a doctor's office where samples were sent to LabCorp for testing. On information and belief, LabCorp provided Plaintiff Finch's Personal Information to AMCA as part

of its bill collections practice. Mr. Finch reviewed LabCorp's privacy policies on a screen at the time she received the laboratory services, but was not provided a hard copy. On or about July 12, 2019, Plaintiff Finch received a data breach notification letter from LabCorp. On or around July 22, 2021, his CashApp account was hacked and $50 was withdrawn via a bank debit card. Mr. Finch had to cancel his bank-issued debit card and obtain a new card. He was able to make a claim and the issuing bank refunded the $50 that was fraudulently taken from the account. Mr. Finch received a pre-paid debit Mastercard in the mail from an online bank that he did not request. He never activated the card or ever deposited funds onto the account. 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. Mr. Finch values his privacy. Had he been informed that LabCorp was going to share his personal information with a debt collection agency that had insufficient data security measures, he would never have continued to use the LabCorp services. Plaintiff Finch's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

KENTUCKY

26. 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 at a LabCorp lab facility 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. Mr. Rothwell has had an uptick in suspicious and highly threatening phishing emails in the last two years. For example,

in one email that attempted extortion, the "APT Hacking Group" claimed to have gained access to his devices, to be tracking his internet activities and even claimed to have recorded videos of him. The hacker threated to share sensitive personal data with his friends, family and coworkers unless he transferred Bitcoin to a Bitcoin wallet address. 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. Mr. Rothwell values his privacy. Had he been informed that LabCorp was going to share his personal information with a debt collection agency that had insufficient data security measures, he would never have continued to use the LabCorp services. Plaintiff Rothwell's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

MARYLAND

27. 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, both at a LabCorp lab facility and through a doctor's office where samples were sent to LabCorp for testing. On information and belief, LabCorp provided Plaintiff Kaplan's Personal Information to AMCA as part of its bill collections practice. Ms. Kaplan reviewed LabCorp's privacy policies at the time she received the laboratory services. On or about July 20, 2019, Plaintiff Kaplan received a data breach notification letter from LabCorp. In 2021, Ms. Kaplan discovered that her credit was pulled for something that she did not cause or authorize. She has received alerts from fraud monitoring products, but does not remember the details. 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. Ms. Kaplan values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Kaplan's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

MASSACHUSETTS

28. 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 at a LabCorp lab facility and, on information and belief, LabCorp provided Plaintiff Shulman's Personal Information to AMCA as part of its bill collections practice. Ms. Shulman believes she reviewed LabCorp's privacy policies at the time she received the laboratory services, but is not absolutely certain. 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. Ms. Shulman believes that she closed one credit card account following fraudulent charges in around May or June 2019. On or around May 24, 2019, two fraudulent international charges from Brazil appeared on one of Ms. Shulman's credit cards. She had to spend time dealing with the credit card company to address the fraud and close the account. On or around June 14, 2019, fraudulent charges appeared on another one of Ms. Shulman's credit cards. Ms. Shulman recently received a suspicious notice in the mail regarding insurance on a car that she previously owned, threatening that if she did not pay money, she would be in trouble, where neither she nor anyone in her family still owned the car. She believed this was attempted fraud. 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. Ms. Shulman values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Shulman's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

MISSISSIPPI

29. 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, both at a LabCorp lab facility and through a doctor's office where the doctors sent samples to LabCorp for testing. On information and belief, LabCorp provided Plaintiff Spencer's Personal Information to AMCA as part of its bill collections practice. Mr. Spencer reviewed LabCorp's privacy policies at the time he received the laboratory services. 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. Someone set up a fraudulent eBay seller account in his name, resulting in Mr. Spencer receiving charges of $14 per week for about a month using his credit card information. Mr. Spencer was forced to order a new credit card and cease using that credit card account that incurred the fraudulent charges. eBay is trying to charge him $500 for something which he did not purchase or authorize and that fraudulent charge has not yet been resolved. Mr. Spencer has received an alert from a credit monitoring service notifying him that someone is checking his credit score,

when he has not engaged in any activity requiring credit inquiries. 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. Mr. Spencer values his privacy. Had he been informed that LabCorp was going to share his personal information with a debt collection agency that had insufficient data security measures, he would never have continued to use the LabCorp services. Plaintiff Spencer's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

30. 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, both at a LabCorp lab facility and through a doctor's office where the doctors sent the samples to LabCorp for testing. On information and belief, LabCorp provided Plaintiff Thomas's Personal Information to AMCA as part of its bill collections practice. Mr. Thomas would have reviewed LabCorp's privacy policies, if he was given them at the time he received the laboratory services. 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. Someone used his card to buy a coat at Guess in Tennessee and something else in Mississippi that appeared as charge from Coca-Cola. His bank was able to block the transactions before they went through. Plaintiff Thomas also received an email that his Personal Information was on the dark web. Mr. Thomas was informed by CreditWise that his password was compromised and 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. Mr. Thomas values his privacy. Had he been informed that LabCorp was going to share his personal information with a debt collection agency that had insufficient data security measures, he would never have continued to use the LabCorp services.

NEW JERSEY

31. 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, both at a LabCorp lab facility and through the state community health center where the doctors sent the samples to LabCorp for testing. 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. Mr. Lebon recalls receiving a notice that someone attempted to open a credit card using his name, but does not recall the details. Mr. Lebon recalls having fraudulent charges appear on his credit card, but does not recall the details. Mr. Lebon recalls that incidents have appeared on his credit reports that he did not cause, but cannot recall the details. 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. Mr. Lebon values his privacy. Had he been informed that LabCorp was going to share his personal information with a debt collection agency that had insufficient data security measures, he

would never have continued to use the LabCorp services. Plaintiff Lebon's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

NEW YORK

32. 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, she believes, either at a LabCorp lab facility or through a doctor's office where the doctors sent the samples to LabCorp for testing. On information and belief, LabCorp provided Plaintiff Gadero's Personal Information to AMCA as part of its bill collections practice. Ms. Gadero recalls signing something at the bottom of the paperwork, but she does not recall if it was the LabCorp's privacy policies. 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. Beginning in or around May 2019, Plaintiff Gadero suffered fraudulent activity on her bank account three times. Ms. Gadero believes that the second incident occurred in June 2019 and again in one or two months after that. She had to change her bank debit card three times after reviewing the charges and seeing charges from another state that she did not make. Her bank closed the account and sent her new cards on each occasion. This caused delays in being able to pay her bills, but she was able to contact the necessary billing agencies to inform them of the situation, so she would not incur late charges. 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. Ms. Gadero is so worried about her accounts being hacked that she checks her accounts at least once a

day. She is so worried about fraud that she has stopped using credit cards and prefers to make purchases with cash. Ms. Gadero values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services.

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, both at a LabCorp lab facility and through a doctor's office where the doctors sent the samples to LabCorp for testing. On information and belief, LabCorp provided Plaintiff Wallach's Personal Information to AMCA as part of its bill collections practice. Ms. Wallach's general practice is to read everything she receives before she signs. Since the privacy policies were likely provided with the HIPAA documents, she believes she reviewed them. On or about June 6, 2019, Plaintiff Wallach received a data breach notification letter from AMCA. Ms. Wallach received emails notifying her of attempts to change her passwords on various accounts and asking for her to confirm her identity, when she had not attempted to change the passwords. 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. Ms. Wallach had received many notifications that her confidential information has been found on the dark web, including her email address, password, street address and date of birth. She actively monitors CreditWise (through Capital One), Credit Karma, ihavebeenpwned and a monitoring service offered through Allstate. She has received approximately 40 dark web alerts from CreditWise since 2019. These are all free credit monitoring services that allow internet users to check whether their personal data has been compromised by data breaches. 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. 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. Ms. Wallach values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Wallach's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

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 through a doctor's office where the doctors sent the samples to LabCorp for testing. 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. Someone charged $500 in car parts on Ms. Vazquez's eBay account. She disputed the charge. Ms. Vazquez has received numerous notices from Credit Karma that her confidential information was found on the dark web. 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. Ms. Vazquez values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Vazquez's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

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 through her doctor's office in Greensboro, North Carolina, which sent samples to LabCorp for testing. On information and belief, LabCorp provided Plaintiff Wrenn's Personal Information to AMCA as part of its bill collections practice. Ms. Wrenn believes that she signed a document related to LabCorp's privacy policy. 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 cause or authorize. A credit card company sent her a letter saying that her request for the credit card was denied, when she had not applied for the credit card. This incident negatively impacted her credit score. Ms. Wrenn then started freezing her credit, which was inconvenient and caused other incidents. For example, when she tried to refinance her car with her credit union in July 2019, she forgot to "unfreeze" her credit, so the credit union was not able to run the credit check and she was delayed in obtaining the refinancing. Within the past year, Ms. Wrenn received approximately two alerts from her credit monitoring services, Credit Karma, Credit Sesame and/or Wallethub, related to someone trying to open an account using her name. She had not opened such account and she did not authorize it. Starting in August 2019 and continuing through early 2020, Ms. Wrenn received spam emails supposedly from Amazon saying that she needed to submit more information to finalize her order,

however, at that time she did not have an Amazon account. 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. Ms. Wrenn values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Wrenn's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

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 at three different LabCorp lab facilities in Columbus, Ohio. On information and belief, LabCorp provided Plaintiff Harris's Personal Information to AMCA as part of its bill collections practice. Ms. Harris believes that she reviewed LabCorp's privacy policies at the time she received the laboratory services on some occasions. Ms. Harris On or about July 12, 2019, Plaintiff Harris received a data breach notification letter from LabCorp. Ms. Harris is so worried about credit card and debit card fraud, that she keeps her cards "locked" until she needs to make a purchase with a card and then unlocks the card, makes the purchase and then locks it back after the payment clears. Ms. Harris has experienced a major uptick in spam phone calls beginning around May or June 2021 when she started receiving multiple spam calls per day. On January 24, 2022, she received an alert from a fraud monitoring service, CreditWise (through Capital One), that her social security number, driver's license number and state, first and last name and phone number were found on the "dark

web." Ms. Harris received a bill in October 2019 from Grant Medical Hospital for $750 that she believes she did not incur. She is still working with that hospital to straight out the issue. Ms. Harris' email account was compromised and she has had to change her passwords several times. 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. In the past, 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. Ms. Harris is so worried about identity theft at this point, that she uses several credit monitoring services and has spent approximately 8 hours per week setting up the monitoring of her accounts and tracking her information. Ms. Harris values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Harris' personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

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 through her doctor's office, which sent samples to LabCorp for testing, and then she would subsequently receive the bills from LabCorp. On information and belief, LabCorp provided Plaintiff Thrower's Personal Information to AMCA as part of its bill collections practice. On or about July 12, 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 or cause. Ms. Thrower requested credit bureau reports from Equifax, Experian and Trans Union in or around early 2019 and upon review of the credit inquiries in those reports discovered

numerous credit inquiries that she did not cause and believes they were directly related to the AMCA/LabCorp data breach. Those original 2019 credit bureau reports were inadvertently discarded along with other items when her home was undergoing upgrades and repairs. However, in November of 2020, she again requested credit bureau reports from Equifax, Experian and Trans Union and the later reports still contained some of the 2019 unauthorized credit inquiries and new ones that she did not cause. In April 2021, she reviewed the November 2020 credit bureau reports and identified unauthorized credit inquiries on the Equifax report on page 31 from Credit One Bank, NA and on page 32 from Big Picture Loans Ltd; from the Experian report on page 7 from EDS/Finwise Bank & Trust and on page 8 from Midnight Velvet, Clarity, EDS/Finwise Bank & Trust, Lexis Nexis, Rise, Monroe & Main; and from the Trans Union report on page 8 from CB Indigo, Finwise, Arrowhead, Advance Applied Data Finance and Continental Fin Co. 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. Ms. Thrower values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would have requested that her doctor's office not continue to use the LabCorp services. Plaintiff Thrower's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

PENNSYLVANIA

38. 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 through a doctor's office where the doctor sent samples to LabCorp for testing by

mistake. He took the LabCorp bill to the doctor's office to complain. The doctor's office told him it was a mistake, but they would not do anything about it. 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. In about the Summer of 2021, Mr. Judelsohn received an alert from Discover's fraud monitoring product informing him that someone in the Midwest had tried to charge a large amount of gas on his credit card. 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. Mr. Judelsohn values his privacy. Had he been informed that LabCorp was going to share his personal information with a debt collection agency that had insufficient data security measures, he would never have continued to use the LabCorp services. Plaintiff Judelsohn's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

TEXAS

39. 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 at a LabCorp lab facility and, on information and belief, LabCorp provided Plaintiff Cuvillier's Personal Information to AMCA as part of its bill collections practice. Ms. Cuvillier reviewed LabCorp's privacy policies at the time she received the laboratory services. On or about July 26, 2019, Plaintiff Cuvillier received a data breach notification letter from LabCorp. Ms. Cuvillier has had

to close a credit card account and open a new one with a new number, but does not recall the circumstances. Ms. Cuvillier had received increased spam calls and receives them almost daily. She has experienced attempted theft of her highly confidential information with the spam caller telling her that her social security number has been breached and that she needs to provide her social security number in order to maintain security. She receives similar spam emails daily. 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. Ms. Cuvillier values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Cuvillier's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

WISCONSIN

40. 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 through a doctor's office where the doctor sent samples to LabCorp for testing. 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. Ms. Allende values her privacy. Had she been informed that LabCorp was going to share her personal information with a debt

collection agency that had insufficient data security measures, she would never have continued to use the LabCorp services. Plaintiff Allende's personal information was also discovered for sale on a dark web marketplace, along with other victims of the Data Breach.

DEFENDANT

41. 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's Data Protection Obligations

42. 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.

43. 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."[3]

44. 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."[4] LabCorp's "most frequently requested tests include blood chemistry analyses, urinalyses, blood cell counts, thyroid tests, Pap tests, hemoglobin A1C, prostate-specific

[3] LabCorp Form 10-K for fiscal year ended Dec. 31, 2018, at 7, https://www.sec.gov/Archives/edgar/data/920148/000092014819000033/lh10-k2018.htm.

[4] *Id.* at 9.

antigen (PSA), tests for sexually transmitted diseases, hepatitis C (HCV), tests, vitamin D, microbiology cultures and procedures, and alcohol and other substance-abuse tests."[5] LabCorp performs this core group of tests in its major laboratories.[6]

45. LabCorp operates a network of "Patient Service Centers" ("PSCs") throughout the United States, at which it performs specimen collection services for patients, such as Plaintiffs and Class Members.[7] 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]."[8]

46. 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 ordering 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.[9]

---

5 *Id*.

6 *Id*.

7 *Id*. at 5.

8 *Id*. at 8.

9 LabCorp, *What to Expect,* https://www.labcorp.com/labs-and-appointments/what-to-expect (last visited Mar. 28, 2022).

47. LabCorp promises that its "staff will make the specimen collection process as safe, quick, and comfortable as possible while safeguarding your dignity and privacy."[10]

48. 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.[11]

49. 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.[12]

50. 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.[13]

51. LabCorp is an entity 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.

---

[10] *Id.*

[11] *See* LabCorp, *Frequently Asked Questions: Billing & Insurance*, https://www.labcorp.com/frequently-asked-questions/patient/11/all/ (last visited Mar. 28, 2022).

[12] LabCorp Form 10-K at 12 *supra* n.3.

[13] U.S. Dep't of Health and Human Services, Office for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Mar. 28, 2022).

52. 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.

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

54. HIPAA requires that LabCorp implement appropriate safeguards for this information.

55. HIPAA also requires that LabCorp provide every patient it treats, including Plaintiffs and the putative Class Members with a privacy notice. LabCorp's "HIPAA Notice of Privacy Practices" acknowledges their legal requirement to maintain the privacy of patients' PHI, and states it is "are committed to the protection of your PHI."[14] LabCorp states that "LabCorp is required to provide patient notification if it discovers a breach of unsecured PHI."[15]

56. HIPAA mandates that a covered entities such as LabCorp may disclose PHI to a "business associate," 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.[16]

---

[14] LabCorp, HIPAA Notice of Privacy Practices, https://www.labcorp.com/hipaa-privacy/hipaa-notice-privacy-practices (last visited Mar. 30, 2020).

[15] *Id*.

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

57. HIPAA further requires that LabCorp 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.

58. AMCA is a "business associate" of LabCorp under HIPAA.

59. The operative agreement between LabCorp and AMCA relevant to this case, the *Patient Collection Agency Agreement*, that the parties initially entered into on [redacted] defined AMCA as [redacted] This agreement also provided LabCorp [redacted].[17]

60. Moreover, according to the *HIPAA Business Associate Addendum* to the agreement, AMCA was required to use [redacted] and maintain a [redacted] in place to [redacted].[18] The addendum also provided that AMCA must [redacted].[19]

61. LabCorp provided AMCA with Personal Information regarding LabCorp's patients in order to facilitate the bill-collection process.

62. The *HIPAA Business Associate Addendum* assumes [redacted] Furthermore, documents from AMCA also reveal that AMCA explicitly contemplated in the templates it provided to LabCorp relating to customer accounts that

---

17 *See* RMCB-AG-00001467-77.

18 RMCB-AG-00001472.

19 RMCB-AG-00001473.

20 LC000677.

LabCorp should include referring physician information among the several categories of requested PII and PHI relating to those accounts.[21] Moreover, in one internal AMCA email, an AMCA employee stated that she "printed the HCFAs" for a patient who appeared to live in California, and she then sent the forms along with other attachments to someone else at AMCA."[22] "HCFA" pertains to a common form issued by the Health Care Finance Administration and used by medical providers in the context of insurance claims and includes, among other things, the patient's medical diagnosis, procedures, hospitalization dates, dates of service, and healthcare provider name.[23]

63. LabCorp's admissions to regulators demonstrate, beyond any serious doubt, that LabCorp breached its duties to Plaintiffs and Class members under HIPAA. LabCorp expressly admitted to regulators that it [redacted][24]

64. These patients' Personal Information was stored in the AMCA systems that were compromised by the Data Breach.[25]

65. The patients' Personal Information LabCorp provided to AMCA, including Plaintiffs' and Class Members', included PII and PHI, such as the first and last name, date of birth,

---

[21] *See, e.g.*, AMCAPROD00698864-65 (AMCA stated that they needed basic patient information (name, date of birth, address, etc.) along with "Provider Name/Referring Physician or location," and AMCA provided a spreadsheet called "Basic Account Data in Placement Files for Collections" with those as fields to fill in (along with "Referring Physician or Location Number").

[22] AMCAPROD00257103-107.

[23] *See* Health Insurance Claim Form, https://www.cms.gov/Medicare/CMS-Forms/CMS-Forms/downloads/cms1500.pdf.

[24] *See* LC001019.

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

SSN, address, telephone number, date of service, healthcare provider, testing codes, and account balance information.[26]

66. Upon information and belief, based upon documents produced by AMCA, LabCorp also provided ICD Codes set forth in the International Classification of Diseases Diagnosis and Procedure Codes, which are defined by the Centers for Disease Control and Prevention ("CDC") as "the official system of assigning codes to diagnoses and procedures associated with hospital utilization in the United States."[27]

67. ICD Codes are assigned to every disease and can be used to relay and track conditions and diseases in a standardized fashion. The CDC refers to ICD Codes as "the cornerstone of classifying diseases, injuries, health encounters and inpatient procedures in morbidity settings. U.S. public health officials at the federal, state, and local level rely on the receipt of ICD-9-CM coded data from HIPAA-covered entities to conduct many disease-related activities."[28] The CDC notes that:

- **A primary user** of ICD codes includes health care personnel, such as physicians and nurses, as well as medical coders, who assign ICD-9-CM codes to verbatim or abstracted diagnosis or procedure information, and thus are originators of the ICD codes. ICD-9-CM codes are used for a variety of purposes, including statistics and for billing and claims reimbursement.

---

[26] *Id.*; *see also* 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. 7:19-bk-23185, ECF No. 2 (Bankr. S.D.N.Y. June 17, 2019).

[27] Centers for Disease Control and Prevention, International Classification of Diseases, Ninth Revision, Clinical Modification (ICD-9-CM), https://www.cdc.gov/nchs/icd/icd9cm.htm#:~:text=ICD%2D9%2DCM%20is%20the,10%20for%20mortality%20coding%20started (last visited March 21, 2022).

[28] Centers for Disease Control and Prevention, International Classification of Diseases, (ICD-10-CM/PCS) Transition - Background, https://www.cdc.gov/nchs/icd/icd10cm_pcs_background.htm (last visited March 21, 2022).

- **A secondary user** of ICD-9-CM codes is someone who uses already coded data from hospitals, health care providers, or health plans to conduct surveillance and/or research activities. Public health is largely a secondary user of coded data.[29]

68. ICD Codes can be used to identify information relating to an individual's medical history, mental or physical condition, and treatment. Indeed, there are numerous publicly available online databases that allow anyone with an internet connection to quickly and easily look up specific diagnosis or condition information associated with an ICD Code.[30] Accounting for the specificity reflected in the coding process, the most recent revision of the ICD Code contains more than 72,000 diagnosis codes that represent conditions and diseases, related health problems, abnormal findings, signs and symptoms, injuries, external causes of injuries and diseases, and social circumstances.[31] For example, ICD-9-CM Code 042 means a conclusive diagnosis of symptomatic HIV infection. ICD-9-CM Code 795.71 means inconclusive or nonspecific HIV test results, including inconclusive HIV test findings in infants. ICD-9-CM Code 054.9 means a diagnosis of herpes simplex without mention of complication, while ICD-9-CM Code 054.11 means herpetic infection of the penis.

69. ICD Codes are protected health information under HIPAA in that they "[r]elate[] to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." 42 U.S.C. § 160.103

---

[29] *Id*.

[30] *See, e.g.*, ICD Code Lookup, https://icdcodelookup.com/icd-10/codes; ICD10Data.com, https://www.icd10data.com/; Codify by AAPC, https://www.aapc.com/codes/icd-10-codes-range/.

[31] Codify by AAPC, What is ICD-10?, https://www.aapc.com/icd-10/ (last visited March 21, 2022).

70. AMCA collected and maintained the Personal Information LabCorp provided to AMCA in its own computer systems. These same AMCA systems were compromised in the Data Breach.

71. In addition, AMCA also obtained 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.

72. During its bankruptcy proceedings in the United States Bankruptcy Court in the Southern District of New York, AMCA 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, SSNs, 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."[32] AMCA 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."[33]

73. In addition, as part of AMCA's billing collection services for Defendant, Plaintiffs furnished Personal Information to AMCA, which AMCA subsequently stored.

B. How the Data Breach Occurred

74. From at least August 1, 2018 through March 30, 2019, an unauthorized user or users gained access to the AMCA system that contained Personal Information obtained from various entities, including Defendant LabCorp, as well as information that AMCA collected itself. [redacted]

[32] Declaration of Russell H. Fuchs, *supra* n.26, at ¶13.

[33] *Id.*

[redacted] and the intrusion may have covered a longer period.

75. Upon information and belief, and based on the limited documents produced to date, the threat actors were able to exploit easily recognizable vulnerabilities in the AMCA IT infrastructure to perpetrate the Data Breach.

76. [redacted]

77. [redacted]

78. Specifically, the evidence shows that [redacted][35] Web shells are pieces of code placed on a web application server to provide an interface for a remote attacker to execute commands. An attacker attaches an executable script, here in the [redacted] to the web server and the script

[34] RMCB-AG-195 (emphasis added).

[35] *Id.*

searches for vulnerabilities in a web server's systems. The web shell can also execute commands and upload and download files.

79. Web shells are only possible if the web application or server contain vulnerabilities such as insecure or poorly written code, a misconfiguration, credentials that are unencrypted, a lack of security patching, or minimal segmentation between different areas in a network. Moreover, web shells leave contemporaneous evidence of their activities, referred to as "noise," [redacted] Additionally, commercial scanning tools and anti-virus software can detect and prevent the installation of web shells, [redacted]

80. [redacted]

81. Specifically, threat actors found the following [redacted][36]

a. [redacted]

b.

c.

d.

[36] RMCB-AG-197-198.

82. [redacted] In March 2020, amcaonline.com still showed an unpatched version of Apache and an unpatched version of MySQL.

83. [redacted] This is a basic feature of IT security. It is well known in the industry that threat actors learn of vulnerabilities in IT systems and exploit them if they are not patched, and even basic IT security requires constant patching and updating as potential vulnerabilities become known. [redacted]

84. As a result, AMCA's system was not a difficult system to attack; threat actors could have discovered the vulnerabilities through simple open source tools from the Internet and commercially available hacking tools.

85. Once threat actors were inside AMCA's systems, they were not detected in part because:

a. [redacted]

b. [redacted]

86. Even if an attacker is able to get into AMCA's systems via a web shell, an appropriate IT system needs to provide additional security to protect the most important (and desirable/valuable) information. This includes taking steps to segregate the most important systems from the rest of the system and limiting who can access these systems. [redacted]

[redacted]

87. [redacted]

[redacted] Again, LabCorp should have known this and, in fact, would have known this had it exercised its oversight responsibilities of AMCA under HIPAA and its contracts with AMCA that LabCorp admits it did not do.

88. [redacted]

[redacted]

89. [redacted][37]

90. [redacted]

91. [redacted]

92. [redacted]

93. At no point did AMCA discover the threat actors—not upon entry, not when they traversed the system, not when they overrode the requirement for a user to authenticate themselves, and not when they exfiltrated files.

---

[37] RMCB-AG-195.

[38] RMCB-AG-196.

C. AMCA's 2019 Audit Revealed Serious Vulnerabilities that It Did Not Remediate

94. [redacted]

95. [redacted] In layman's terms, this meant that compromising the public-facing web server allowed threat actors to compromise the underlying, non-publicly facing, database server containing the PII and PHI at issue in this case.

96. [redacted]

97. [redacted]

[redacted]

D. Threat Actors Sold Class Members' Personal Information on the Dark Web

98. Following the Data Breach, there was evidence that the exfiltrated PII and PHI was available for sale on the dark web and was, in fact, already being used to commit fraud.

99. Specifically, in November 2018, after forensic evidence proved that files were exfiltrated by threat actors, AMCA was contacted by GlobalOnePay who informed AMCA that [redacted][39] This was done via a "common point of purchase" which is a way for credit card banks to trace fraud associated with the use of their cards.

100. At that time, Conformance Tech noted that there were [redacted][40]

101. [redacted]"[41]

[39] RMCB-AG-25.

[40] AMCAPROD138907.

[41] *Id.*

102. [redacted]

103. [redacted]

104. At the end of February 2019, Gemini Advisory, a New York-based company that works with financial institutions to monitor the sale of consumer information on underground markets, ***identified a large number of compromised AMCA patient information for sale on the dark web***.[44] As reported on May 10, 2019 by DataBreaches.net:

> On February 28, 2019, Gemini Advisory identified a large number of compromised payment cards while monitoring dark web marketplaces. Almost 15% of these records included additional personally identifiable information (PII), such as dates of birth (DOBs), Social Security numbers (SSNs), and physical addresses. A thorough analysis indicated that the information was likely stolen from the online portal of the American Medical Collection Agency (AMCA), one of the largest recovery agencies for patient collections. Several financial institutions also collaboratively confirmed the connection between the compromised payment card data and the breach at AMCA.[45]

---

[42] AMCAPROD00215349.

[43] AMCAPROD1117103.

[44] Stas Alforov & Christopher Thomas, *AMCA Breach May be Largest Medical Breach in 2019*, GEMINI ADVISORY (June 4, 2019), https://geminiadvisory.io/amca-largest-medical-breach/.

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

105. Gemini's additional research revealed AMCA's exposure window had lasted for at least ***seven months*** beginning in September 2018.[46]

106. The combination of AMCA-related PII/PHI being for sale on the dark web and the common point of purchase notifications that AMCA received definitively shows that the threat actors, after exfiltrating PII and PHI from AMCA's systems, sold the information on the dark web and purchasers of that information subsequently committed credit card fraud.

107. On March 1, 2019, Gemini Advisory attempted to notify AMCA of the data exposure but received no response. Gemini Advisory then contacted federal law enforcement who reportedly followed-up with AMCA.[47]

108. Following notification from law enforcement, AMCA's payment portal became unavailable for weeks.[48]

109. In its notice to patients affected by the breach, AMCA claims it learned of the unauthorized access on March 20, 2019. Yet LabCorp failed to take any steps to notify patients whose Personal Information was affected until months later, initially only doing so through an SEC filing.

110. There are strong indications that the Personal Information exfiltrated from AMCA's database is still being offered for sale on underground markets. A compiled list containing the information of more than 60 individuals from varying geographic regions and demographics who had their information stored on AMCA's database was searched across dark web markets notorious for selling confidential personal information acquired from threat actors

---

[46] *Id.*

[47] *Id.*

[48] *Id.*

and malicious threat actors. Of this sample, ***more than 87%*** had their information offered for sale by ***two single vendors*** on just one popular dark web market. It is highly unlikely that information associated with such a significant percentage of the sample would be available through two vendors unless the data was obtained from the same breach – a significant indication that ***all*** Plaintiffs and Class Members had their Personal Information accessed, exfiltrated, and then disseminated by unauthorized parties. Given the vastness of the dark web, there is high probability that each Plaintiff's and Class Member's data is available for sale.

E. LabCorp Announces the Data Breach

111. 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 United States Department of Health and Human Services ("HHS") in 2019.[49] As of 2019, 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.[50]

112. 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.[51]

---

[49] *Breach Portal*, *supra* n.13; *see also* HIPAA JOURNAL, *August 2019 Healthcare Data Breach Report* (Sept. 23, 2019), https://www.hipaajournal.com/august-2019-healthcare-data-breach-report/.

[50] Jessica Kim Cohen, *July-reported healthcare breaches exposed 22 million people's data*, MODERN HEALTHCARE (Aug. 9, 2019), https://www.modernhealthcare.com/cybersecurity/july-reported-healthcare-breaches-exposed-22-million-peoples-data.

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

113. 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.
>
> * * *
>
> 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."[52]

114. 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.

115. 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

[52] Brian Krebs, *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, *supra* n.46.

> information that was provided by the consumer to AMCA (for those who sought to pay their balance).[53]

116. 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 provided LabCorp a list of the affected LabCorp consumers or more specific information about them."[54]

117. 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,"[55] LabCorp later disclosed that SSNs and health insurance information may have been included as well.[56]

118. 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.**[57]

---

[53] LabCorp Form 8-K, *supra* n.25.

[54] *Id.*

[55] *Id.*

[56] LabCorp Form 10-Q (Aug. 8, 2019), https://ir.labcorp.com/static-files/fc907b06-523a-4ff1-9fee-3985cb2076b6.

[57] *Id.* (emphasis added).

119. 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.[58] LabCorp did not disclose this fact either in its August 8, 2019 filing with the SEC or on its website.[59]

F. LabCorp Failed to Exercise Due Care in Contracting with AMCA

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

121. While limited in nature, discovery to date in this case reveals that LabCorp may have not, and perhaps more likely, did not conduct *any* due diligence and risk analysis of AMCA's data security preceding the Data Breach.

122. Despite being contractually empowered to audit AMCA through the duration of the parties' operative agreement, on September 22, 2016, LabCorp personnel visited AMCA offices for the ***first*** time and, according to AMCA, "[p]art of this visit will be a discussion/audit of [AMCA's] internal policies."[60]

123. In January 2017, AMCA submitted a report to the PCI Security Standards Council. Zach Raxter, AMCA's Director of IT and Security, completed the PCI self-attestation of compliance and Jeff Wollman signed the document in April 2017.[61] In the report, AMCA self-attests to compliance with operative PCI standards governing data security,[62] but it is unknown

---

[58] *Breach Portal*, *supra* n.13.

[59] *See* LabCorp Form 10-Q, *supra* n.51 (emphasis added); *see also* Information about the AMCA Data Security Incident, *supra* n.46.

[60] AMCAPROD00247761.

[61] AMCAPROD00723845.

[62] AMCAPROD00723845.13

whether this attestation was ever transmitted to LabCorp, whether LabCorp did any follow up to verify AMCA's answers in the report, or whether these attestations comport with LabCorp's knowledge from the September 2016 site visit. LabCorp's failure to produce any documentation concerning its ***own*** due diligence over AMCA's PCI compliance, a subject that the purported agenda for the September 2016 visit to AMCA should have reasonably included, remains both curious and suspicious at this point in the litigation.

124. The work of an outside auditor corroborates that inference. On or about April 4, 2019, LabCorp commissioned Crowe LLP ("Crowe") to conduct analyses of LabCorp's vendor risk management programs. Crowe included its analysis and conclusions in a report submitted to LabCorp on or around October 11, 2019. In its report, Crowe found, *inter alia,* that [redacted][63]

125. LabCorp's document production to date thus far demonstrates no oversight of AMCA's compliance with either PCI standards or HIPAA confidentiality obligations. AMCA's documents demonstrate that LabCorp knew or at a minimum was reckless in not knowing about numerous significant, systemic weakness in AMCA's data security (had LabCorp bothered to look).

126. In addition to its customers' PII and PHI, AMCA stored their credit card and CVV2 numbers in its database unencrypted, in violation of prevailing industry standards.[64] Moreover,

---

[63] LC0000734-735.

[64] While LabCorp contends that AMCA collected Plaintiffs' and Class Members' financial information directly, rather than receiving it from LabCorp, it was ***LabCorp's*** obligation under HIPAA and its contractual obligations with AMCA to ensure that such information was secure.

AMCA's documents contain additional evidence demonstrating LabCorp's awareness of the following:

a. that files containing patient PII and PHI were transmitted by LabCorp to AMCA via an outdated File Transfer Protocol ("FTP") connection throughout 2016 and 2017, and likely beyond, as well as via regular unencrypted email;

b. that both AMCA and LabCorp transmitted sensitive log-in credentials of the kind used to infiltrate AMCA's system via regular mail when a secure e-mail system was available to both;

c. that both AMCA and LabCorp regularly transmitted extensive PII and PHI of its customers via unencrypted and non-secured email. LabCorp and AMCA employed this practice despite the availability of FTP transfer and a secured e-mail system between LabCorp and AMCA; and

d. that LabCorp took a very lax approach to information technology ("IT") security and data management.

Despite LabCorp's awareness of the foregoing issues, it failed to act.

127. Other information confirms that LabCorp should not have entrusted AMCA with Plaintiffs' and Class Members' Personal Information. AMCA's bankruptcy filings indicate how thinly capitalized the company was and how insignificant its 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.

128. 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.

129. 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

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.[65] The fact that it took AMCA at least 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 conducted due diligence on AMCA's data security practices (or lack thereof) before providing AMCA sensitive PHI and PII.

130. 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.[66]

131. AMCA did not need access to Plaintiffs' PHI to collect payments. Instead, AMCA only needed the name of the vendor (LabCorp), the invoice number, amount owed, and date of service to perform its collection services. But Defendant nevertheless regularly provided full

[65] FIREEYE, *M-Trends 2019: FireEye Mandiant Services Special Report*, https://content.fireeye.com/m-trends/rpt-m-trends-2019 (last visited Mar. 28, 2022).

[66] *Id.*

account information that included PHI, apparently because it was more expedient than providing the narrower data set to AMCA.

132. AMCA maintained PHI and PII for closed files and failed to routinely destroy or archive inactive records. Defendant would have discovered this had it exercised adequate oversight over its business associates and audited the data security protocols utilized by AMCA.

133. 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.

134. 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 of PCI DSS.[67]

135. 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

[67] *Securing Account Data with the PCI Point-to-Point Encryption Standard v2* (June 2015), https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf.

authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[68]

136. 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.

137. 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."[69] However, LabCorp did not learn of the unauthorized access until months later in May 2019.

G. LabCorp Failed to Provide Proper Notice of the Data Breach

138. 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.

---

[68] *Id.*

[69] 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.

139. 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."[70]

140. However, rather than send notice directly, LabCorp relied on AMCA to mail notices to those individuals on its system in June 2019.[71] 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 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.

141. 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.[72] 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 SSNs may have been affected.[73] This limitation means that customers who had other forms of Personal Information taken are not protected. As detailed *infra*, the theft

[70] LabCorp Form 8-K, *supra* n.25.

[71] *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.

[72] Information about the AMCA Data Security Incident, *supra* n.46.

[73] *Id*.

of various forms of Personal Information, not just SSNs 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 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.[74] 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.

142. 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.

143. 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.

H. LabCorp's Violated HIPAA's Requirements to Safeguard Plaintiffs and Class Members' Personal Information

144. Defendant failed to maintain the privacy and security patients PHI and failed to inform patients that their Personal Information was disclosed. Indeed, Defendant violated HIPAA by failing to:

[74] *Id.*

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

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 their workforces, in violation of 45 C.F.R. §164.306(a)(4); and/or

j. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. §164.530(b).

145. Additionally, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance

of reasonable data security practices, which should be factored into all business-related decision making.[75]

146. The FTC's publication *Start With Security*: *A Guide for Business* sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data. Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[76]

147. Additionally, the FTC recommends that organizations limit access to sensitive data, re-quire complex passwords to be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[77]

148. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. §45. Orders

---

[75] FTC, *Start With Security: A Guide for Businesses* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[76] *Id*.

[77] *Id*.

resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[78]

149. Defendant was fully aware of their obligations to implement and use reasonable measures to protect the PII and PHI of LabCorp's patients but failed to comply with these basic recommendations and guidelines that would have prevented the Data Breach from occurring.

I. LabCorp Violated HIPAA's Requirements to Safeguard Data

150. 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.

151. Indeed, LabCorp's entire business depends on patient's entrusting it with their Personal Information. Without patient's Personal Information, LabCorp would not be able to perform any services and certainly would not be able to bill patients and their insurance companies and collect payment for services rendered.

152. That is why 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.

153. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information"

[78] FTC, *Privacy and Security Enforcement*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Mar. 30, 2022).

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.

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

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

156. 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.[79]

157. 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.

158. 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;

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);

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

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).

159. 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.

J. LabCorp Patients' Personal Information Is Highly Valuable

160. 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.[80]

[80] HIPAA JOURNAL, *Healthcare Data Breach Statistics*, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Mar. 30, 2022) ("Our

161. HHS' Office for Civil Rights currently lists all healthcare data breaches since February 27, 2020. Since then, the largest data breach involved 3.5 million victims. The AMCA Data Breach of LabCorp patients, however, involved ***three times*** that number.[81]

162. As early as 2014, the FBI alerted the healthcare industry that it was an increasingly preferred target of threat actors, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (PII)" so that these companies can take the necessary precautions to thwart such attacks.[82]

163. 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."[83]

164. 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."[84]

---

healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past 10 years.").

[81] U.S. Dep't of Health and Human Services, Office for Civil Rights, *Cases Currently Under Investigation* (last visited Mar. 28, 2022).

[82] Jim Finkle, *FBI warns healthcare firms they are targeted by threat actors*, REUTERS (Aug. 20, 2014), http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

[83] 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.

[84] 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-

165. 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 SSNs needed to be provided to debt collectors.[85]

166. 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."[86]

167. 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, SSNs and other Personal Information directly on various dark web sites making the information publicly available.[87]

168. Healthcare data is especially valuable on the black market. Healthcare data is especially valuable on the black market. According to one report, a healthcare data record may be

---

security/third-party-data-breach-hits-quest-diagnostics-with-12-million-confidential-patient-records-exposed/.

[85] *Id.*

[86] *Id.*

[87] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web,* EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/; Charles McFarland et al., *The Hidden Data Economy*, at 3, MCAFEE (Dec. 2015), https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf.

valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[88]

169. According to a *Reuters* investigation that included interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts, medical data for sale on underground markets "includes names, birth dates, policy numbers, diagnosis codes and billing information" which fraudsters commonly use "to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers[.]"[89]

170. According to Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black, "Health information is a treasure trove for criminals [because] by compromising it, by stealing it, by having it sold, you have seven to 10 personal identifying characteristics of an individual."[90] For this reason, a patient's full medical records can sell for up to $1,000 on the dark web, while credit card numbers and SSNs may cost $5 or less.[91]

171. As noted by Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies: "The reason for this price discrepancy – like any other good or service – is perceived value. While a credit card number is easily canceled, medical

---

[88] Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data*, SECURELINK (Feb. 2, 2022), https://www.securelink.com/blog/healthcare-data-new-prize-hackers/.

[89] Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit card*, REUTERS (Sept. 24, 2014), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924.

[90] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.

[91] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information. Once records are stolen, cybercriminals often tap into members of a criminal network on the dark web experienced in drug trafficking and money laundering who are eager to buy medical records to support their criminal activities, such as illegally obtaining prescription medications, filing bogus medical claims or simply stealing the patient's identity to open credit cards and fraudulent loans."[92]

172. LabCorp is well aware that its own data and the data it shares with AMCA contained a treasure trove of material for threat actors 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.

173. 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."

K. LabCorp Has Harmed Plaintiffs and Class Members by Allowing Anyone to Access Their Information

174. 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.

---

[92] Paul Nadrag, *Industry Voices – Forget credit card numbers. Medical records are the hottest items on the dark web*, FIERCE HEALTHCARE (Jan. 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web.

175. Given the sensitive nature of the Personal Information stolen in the Data Breach – including names, mailing addresses, phone numbers, dates of birth, SSNs, 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 – threat actors 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.

176. 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.

177. 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.

178. 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.[93]

179. 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 disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges."[94]

180. While federal law generally limits an individual's liability for fraudulent credit card charges to $50, there are no such protections for a stolen medical identity. According to a 2015 survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft spent an average of $13,500 in out-of-pocket costs to resolve the crime.[95] Frequently, this information was used to obtain medical services or treatments (59%), obtain prescription drugs (56%), or receive Medicare and Medicaid benefits (52%). Only 14% of respondents said that the identity thieves used the information to obtain fraudulent credit accounts, indicating that medical information is a much more profitable market.[96]

---

[93] *Id*.

[94] Declaration of Russell H. Fuchs, *supra* n.26, at ¶16.

[95] *Ponemon Institute, Fifth Annual Study on Medical Identity Theft*, https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 (last visited March 21, 2022).

[96] *Id*. at 9.

181. According to the Ponemon study, "[t]hose who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate."[97]

182. Additionally, the study found that medical identity theft can have a negative impact on reputation as 45% of respondents said that medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions, with 19% responding that they missed out on employment opportunities as a result.[98]

183. Exacerbating the problem, victims of medical identity theft oftentimes struggle to resolve the issue because HIPAA regulations require the victim to be personally involved in the resolution of the crime.[99] In some cases, victims may not even be able to access medical records using their personal information because they include a false name or data points taken from another person's records. Consequently, only 10% of medical identity theft victims responded that they "achiev[ed] a completely satisfactory conclusion of the incident."[100]

184. Moreover, it can take months or years for victims to even discover they are the victim of medical-related identity theft or fraud given the difficulties associated with accessing medical records and healthcare statements. For example, the FTC notes that victims may only discover their identity has been compromised after they:

- Receive a bill for medical services they did not receive;

---

[97] *Id*. at 2.

[98] *Id*. at 14.

[99] *Id*. at 1.

[100] *Id*.

- Get contacted by a debt collector about medical debt they do not owe;
- See medical collection notices on their credit report that they do not recognize;
- Find erroneous listings of office visits or treatments on their explanation of benefits (EOB);
- Receive information from their health plan that they have reached their limit on benefits; or
- Be denied insurance because their medical records show a condition they do not have.[101]

185. Other types of medical fraud include "leveraging details specific to a disease or terminal illness, and long-term identity theft."[102] According to Tom Kellermann, "Traditional criminals understand the power of coercion and extortion. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[103] Long-term identity theft occurs when fraudsters combine a victim's data points, including publicly-available information or data points exposed in other data breaches, to create new identities, open false lines of credit, or commit tax fraud that can take years to remedy.

186. 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

[101] *FTC, Medical Identity Theft FAQs for Health Care Providers and Health Plans*, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last visited March 21, 2022).

[102] *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited March 21, 2022).

[103] *Id.*

also be used for regular purchases (albeit incurring a severe tax penalty). Such information is an "easy target" for criminal actors.[104]

187. As AMCA acknowledged, fraudulent charges have already been linked to the data LabCorp provided to AMCA. LabCorp publicly revealed the exposure of patients' Personal Information only after "a disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges."[105]

188. 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.[106] 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.

189. 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

---

[104] *Id.*

[105] Declaration of Russell H. Fuchs Pursuant to Local Bankruptcy Rule 1007-2 And In Support Of "First Day" Motions, American Medical Collection Agency Bankruptcy Petition #19-23185(RDD), Docket Entry 2 (Bankr. S.D.N.Y.)

[106] IDENTITY THEFT RESOURCE CENTER, *The Aftermath 2017*, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Aug. 9, 2019).

> by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[107]

190. 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.[108]

191. 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,

---

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

[108] *See* CNET, *Study: Medical identity theft is costly for victims*, (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

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.

192. 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.[109]

193. 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.[110]

194. 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

[109] E. Harrell, Ph.D., *Victims of Identity Theft, 2014* U.S. Department of Justice (rev. Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

[110] 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* (June 2007), http://www.gao.gov/new.items/d07737.pdf.

provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[111]

195. 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.

196. 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.

197. 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.[112]

[111] Richard Turner, *Beyond the Bottom Line: The Real Cost of Data Breaches* FIREEYE (May 11, 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html.

[112] Letter from United States Senators Robert Menendez and Cory A. Booker (June 5, 2019), https://www.menendez.senate.gov/imo/media/doc/06.05.19%20LabCorp%20Letter.pdf.

198. 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.[113]

199. 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.[114]

200. Other State Attorneys General, including the Attorneys General of Michigan, Minnesota, and North Carolina, have also launched investigations into the Data Breach.[115]

CLASS ACTION ALLEGATIONS

NATIONWIDE CLASS

201. 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"):

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

---

[113] LabCorp Form 10-Q, *supra* n.51.

[114] The Office of Attorney General William Tong, *Connecticut and Illinois Open Investigation into Quest Diagnostics, LabCorp Data Breach* (June 7, 2019), https://portal.ct.gov/AG/Press-Releases/2019-Press-Releases/CT-AND-IL-OPEN-INVESTIGATION-INTO-QUEST-AND-LABCORP-DATA-BREACH.

[115] Steve Adler, *AMCA Data Breach Tally Passes 20 Million as BioReference Laboratories Added to List of Impacted Entities*, HIPAA JOURNAL (June 17, 2019), https://www.hipaajournal.com/amca-data-breach-tally-passes-20-million-as-bioreference-laboratories-added-to-list-of-impacted-entities/.

202. The Nationwide Class asserts claims under North Carolina law against Defendant for violation of the negligence (Count 1), negligence *per se* (Count 2), breach of confidence (Count 3), invasion of privacy – intrusion upon seclusion (Count 4); and unjust enrichment (Count 5).

STATEWIDE SUBCLASSES

203. 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 6 through 20), 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.

204. 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.

205. **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.

206. **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.

207. **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.

208. **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.

209. **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.

210. **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.

211. **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.

212. **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.

213. 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 I

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

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

215. 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.

216. Defendant knew or should have known that AMCA's systems were vulnerable to unauthorized access and exfiltration by third parties.

217. 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.

218. 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.

219. 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.

220. 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.

221. 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 threat actors.

222. Defendant's duties also arose under HIPAA 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)-(e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

223. 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.

224. 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."

225. 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.

226. 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.

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

228. 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.

229. 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.

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

231. 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 II

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

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

233. 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.

234. 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)-(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.

235. 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.

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

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

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

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

240. 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).

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

242. 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.

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

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

245. 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.

246. 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 III

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

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

248. Plaintiffs and Class Members maintained a confidential relationship with Defendant whereby Defendant undertook a duty not to disclose the Personal Information provided by Plaintiffs and Class Members to Defendant to unauthorized third parties. Such Personal Information was confidential and novel, highly personal and sensitive, and not generally known.

249. Defendant knew Plaintiffs' and Class Members' Personal Information was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreed to protect the confidentiality and security of the Personal Information they collected, stored, and maintained.

250. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' Personal Information in violation of this understanding. The unauthorized disclosure occurred because Defendant failed to implement and maintain reasonable safeguards to protect the Personal Information in their possession and failed to comply with industry-standard data security practices.

251. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

252. As a direct and proximate result of Defendant's breach of confidence, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT IV

INVASION OF PRIVACY – INTRUSION UPON SECLUSION
On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

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

254. Defendant intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their Personal Information to a third party that was unequipped and unable to keep their Personal Information secure.

255. By failing to keep Plaintiffs' and Class Members' Personal Information secure, and disclosing Personal Information to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, *inter alia*:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their Personal Information properly obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their Personal Information from disclosure to unauthorized persons; and

d. enabling the disclosure of their Personal Information without consent.

256. The Personal Information that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial, health, and treatment information.

257. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT V

UNJUST ENRICHMENT[116]

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

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

259. For years and continuing to today, Defendant's business model has depended upon patients entrusting it with their Personal Information. Trust and confidence are critical and central to both the services provided by LabCorp to patients and the billing and collection for such services. Unbeknownst to Plaintiffs and absent Class Members, however, Defendant did not secure, safeguard, or protect patient data and employed deficient security procedures and protocols to prevent unauthorized access to patients' Personal Information. Defendant's deficiencies described herein were contrary to their security messaging.

260. Plaintiffs and absent Class Members engaged LabCorp for services and provided Defendant with, and allowed Defendant to collect, their Personal Information on the mistaken belief that Defendant complied with their duty to safeguard and protect patient Personal Information. Putting their short-term profit ahead of safeguarding Personal Information, and unbeknownst to Plaintiffs and absent Class Members, Defendant knowingly sacrificed security in

[116] Plaintiffs recognize the court's order holding that Plaintiffs failed to state an unjust enrichment claim on the grounds that "there is no [] allegation that Defendants . . . receive any additional value from Plaintiffs Personal Information." ECF No. 283 at 33-34. Plaintiffs have added additional allegations to this Count and otherwise assert it to preserve it for appeal.

an attempt to collect money Defendant believed was owed. Defendant knew that the manner in which they maintained and transmitted patient Personal Information violated their fundamental duties to Plaintiffs and absent Class Members by neglecting well-accepted security to ensure confidential information was not accessible to unauthorized access. Defendant had knowledge of methods for designing safeguards against unauthorized access and eliminating the threat of exploit, but it did not use such methods.

261. Defendant had within its exclusive knowledge at all times relevant and never disclosed that they had failed to safeguard and protect Plaintiffs' and absent Class Members' Personal Information and chose to keep their decision strictly confidential. This information was not available to Plaintiffs, absent Class Members, or the public at large.

262. Defendant also knew that Plaintiffs and absent Class Members expected security against known risks and that they were required to adhere to state and federal standards for the protection of confidential personally identifying, financial, and health information.

263. Plaintiffs and absent Class Members did not expect that Defendant would knowingly insecurely maintain and distribute their Personal Information for debt collection purposes. Likewise, Plaintiffs and absent Class Members did not expect that Defendant would engage a debt collection agent, AMCA, that employed substantially deficient security and fail to undertake any required monitoring or supervision.

264. Had Plaintiffs and absent Class Members known about Defendant's efforts to hide their failure to safely guard and protect Personal Information entrusted to them by Plaintiffs and absent Class Members, Plaintiffs and absent Class Members would not have engaged Defendant to perform any services and would never have provided Defendant with their Personal Information.

265. By withholding the facts concerning the defective security and protection of patient Personal Information, Defendant put their own interests ahead of the very patients who placed their trust and confidence in LabCorp and benefitted themselves to the detriment of Plaintiffs and absent Class Members.

266. As a result of their conduct as alleged herein, Defendant sold more services than it otherwise would have and was able to charge Plaintiffs and Class Members when they otherwise could not have. Defendant was unjustly enriched by charging for and collecting for those services to the detriment of Plaintiffs and absent Class Members.

267. It would be inequitable, unfair, and unjust for Defendant to retain these wrongfully obtained benefits. Defendant's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

268. Defendant's defective security and their unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their private Personal Information.

269. Each Plaintiff and member of the proposed Classes is entitled to restitution and non-restitutionary disgorgement in the amount by which Defendant were unjustly enriched, to be determined at trial.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT VI

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

270. 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.

271. 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.*

272. 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).

273. 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.

274. 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."

275. Defendant is subject to the requirements and mandates of the CMIA and are therefore required to do the following under the CMIA:

a. Ensure that medical information regarding patients is not disclosed or disseminated or released without patients' authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Cal. Civ. Code §§56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101;

b. Not disclose medical information regarding a patient without first obtaining an authorization under Cal. Civ. Code §§56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35 and 56.104;

c. Create, maintain, preserve, and store medical records in a manner that preserves the confidentiality of the information contained therein under Cal. Civ. Code §§56.06 and 56.101(a);

d. Protect and preserve confidentiality of electronic medical information in their possession under Cal. Civ. Code §§56.06 and 56.101(b)(1)(A); and

e. Take appropriate preventive actions to protect confidential information or records from unauthorized release under Cal. Civ. Code §56.36I(2)(E).

276. 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.

277. The medical information compromised included Plaintiff's and California Subclass members' full names, mailing addresses, phone numbers, email addresses, dates of birth, SSNs, and genders, in conjunction with information related to Plaintiff's and California Subclass members' medical treatment, such as tests ordered, ordering physician, and ICD Codes. This information considered in its totality constitutes individually identifiable information regarding a patient's medical history, mental or physical condition, and/or treatment.

278. Due to Defendant's negligent creation, maintenance, preservation and/or storage of Plaintiff's and the California Subclass members' electronic medical information, Defendant allowed Plaintiff's and California Subclass members' individually identifiable medical information to be accessed and actually viewed by at least one unauthorized third party, constituting a release in violation of Cal. Civ. Code §56.101(b)(1)(A).

279. Defendant disclosed "medical information," as defined in CMIA, Cal. Civ. Code §56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code §56.10(a). Plaintiff and California Subclass members did not authorize Defendant's disclosure and release of their Personal Information that occurred in the Data Breach.

280. Defendant's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs' and the California Subclass members' medical information in a manner that preserved the confidentiality of the information contained therein violated the CMIA, Cal. Civ.

Code §§56.06 and 56.101(a). Defendant transmitted patients' confidential medical information in an unencrypted and unredacted format to Defendant's associates which was then accessed, viewed, and exfiltrated by an unauthorized third party or parties, and thus Defendant negligently released medical information concerning Plaintiff and California Subclass members. Accordingly, Defendant's systems and protocols did not protect and preserve the integrity of electronic medical information in violation of the CMIA, Cal. Civ. Code §56.101.

281. 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 their 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 their 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.

282. 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.

283. 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.

284. Plaintiff and California Subclass members were injured and have suffered damages, as described above, from Defendant's unauthorized release of their medical information in violation of Cal. Civ. Code §§56.10 and 56.101, and are therefore entitled to nominal damages of one thousand dollars ($1,000) for each violation under Civil Code §56.36(b)(1) or the amount of actual damages, if any, for each violation under Civil Code §56.36(b)(2).

285. 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 VII

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

286. 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.

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

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

289. Defendant's "unfair" and "fraudulent" acts and practices include omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and

business associates reasonably or adequately secured Plaintiff's and California Subclass members' Personal Information.

290. 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.

291. Defendant engaged in acts of deception and false pretense in connection with its accepting, collecting, securing, and otherwise protecting patient Personal Information and engaged in the following deceptive and unconscionable trade practices, including:

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 comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

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

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.

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

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

294. Plaintiff and California Subclass members conferred a benefit on Defendant – payment for medical services – in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and California Subclass members would not have sought or purchased services from Defendant.

295. 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, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein.

296. 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.

297. 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.

COUNT VIII

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

298. 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.

299. 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.

300. 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."

301. 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."

302. 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.

303. 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 omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and California Subclass members' Personal Information.

304. Defendant's 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.

305. Plaintiff and California Subclass members conferred a benefit on Defendant – payment for medical services – in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and California Subclass members would not have sought or purchased services from Defendant.

306. Had Defendant disclosed to Plaintiffs 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 they 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 California Subclass members' Personal Information as part of the services they provided without advising Plaintiffs and California Subclass members that AMCA's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and California Subclass members' Personal Information. Accordingly, Plaintiff and California Subclass members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered.

307. 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 loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations

alleged herein; 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.

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

309. Plaintiff and California Subclass members 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 KANSAS SUBCLASS

COUNT IX

PROTECTION OF CONSUMER INFORMATION

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

310. 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.

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

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

313. 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).

314. 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).

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

316. 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.

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

COUNT X

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

318. 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.

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

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

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

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

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

324. Defendant engaged in deceptive and unfair acts or practices, including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Kansas Subclass members' Personal Information.

325. Defendant's 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.

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

327. Plaintiff and Kansas Subclass members conferred a benefit on Defendant – payment for medical services – in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and Kansas Subclass members would not have sought or purchased services from Defendant.

328. 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 Kansas Subclass members to reasonably protect their interests, due to their lack of knowledge, K.S.A. §50-627(b)(1)); and

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

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

330. 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.

331. 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 loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; 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.

332. 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 XI

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

333. 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. .

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

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

336. 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).

337. 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).

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

339. 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.

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

COUNT XII

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

341. 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.

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

343. 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).

344. Defendant engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. §367.170, including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Kentucky Subclass members' Personal Information.

345. Defendant's 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.

346. 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.

347. Plaintiff and Kentucky Subclass members conferred a benefit on Defendant – payment for medical services – in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and Kentucky Subclass members would not have sought or purchased services from Defendant.

348. 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.

349. 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, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; 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.

350. 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 XIII

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

351. 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.

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

353. 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.

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

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

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

357. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Md. Code, Com. Law §13-301, including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Maryland Subclass members' Personal Information.

358. Defendant's 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.

359. Plaintiff and Maryland Subclass members conferred a benefit on Defendant – payment for medical services – in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and Maryland Subclass members would not have sought or purchased services from Defendant.

360. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive 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 loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; 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.

361. 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 XIV

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

362. 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.

363. 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."

364. 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).

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

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

367. 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.

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

369. 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."

370. 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."

371. 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).

372. 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).

373. 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.

374. 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.

375. 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 XV

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

376. 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.

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

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

379. 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).

380. 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.

381. 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.

382. 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.

383. 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.

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

385. 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.

386. 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.

387. 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.

388. 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 YORK SUBCLASS

COUNT XVI

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

389. 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.

390. 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 omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Michigan Subclass members' Personal Information.

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

392. Defendant's 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.

393. Plaintiff and New York Subclass members conferred a benefit on Defendant – payment for medical services – in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure

its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and New York Subclass members would not have sought or purchased services from Defendant.

394. 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 loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; 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.

395. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the hundreds of thousands, if not millions, of New Yorkers affected by the Data Breach.

396. 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.

397. 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 PENNSYLVANIA SUBCLASS

COUNT XVII

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

398. 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.

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

400. 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.

401. 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 omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Pennsylvania Subclass members' Personal Information.

402. Defendant's 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.

403. Plaintiff and Pennsylvania Subclass members conferred a benefit on Defendant – payment for medical services – in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and Pennsylvania Subclass members would not have sought or purchased services from Defendant.

404. 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.

405. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices, 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, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; 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.

406. 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 WISCONSIN SUBCLASS

COUNT XVIII

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

407. 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.

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

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

410. 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).

411. 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).

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

413. 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.

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

COUNT XIX

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

415. 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.

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

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

418. 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).

419. 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).

420. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Wis. Stat. §100.18(9), including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Wisconsin Subclass members' Personal Information.

421. Defendant's 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.

422. Plaintiff and Wisconsin Subclass members conferred a benefit on Defendant – payment for medical services – in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and Wisconsin Subclass members would not have sought or purchased services from Defendant.

423. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive 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 loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; 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.

424. 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 requests that the Court enter judgment in their favor and against Defendant, as follows:

A. 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;

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

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

D. 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;

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

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

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

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

I. 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: March 31, 2022

Linda P. Nussbaum
Susan R. Schwaiger
NUSSBAUM LAW GROUP, P.C.
1211 Avenue of the Americas, 40th Floor
New York, New York 10036

Tina Wolfson
Brad King
Theodore W. Maya
AHDOOT & WOLFSON, PC
1016 Palm Avenue

(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

LabCorp Track Co-Lead Counsel

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

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