Exhibit C15

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
Civil Action No.: _____

MOHAMAD MOHAMAD, individually and on behalf of all other persons similarly situated, **Plaintiff,** **v.** **LABORATORY CORPORATION OF AMERICA HOLDINGS,** **Defendant.**	**COMPLAINT-CLASS ACTION (MDNC LR 23.1)** **JURY TRIAL DEMANDED**

Plaintiff, Mohamad Mohamad, by way of Complaint on behalf of himself and others similarly situated, individually and as class representative, alleges and says as follows:

INTRODUCTION

1. This is a class-action Complaint brought by Plaintiff, Mohamad Mohamad ("Plaintiff") on his own behalf and on behalf of all others similarly situated against Defendant Laboratory Corporation of America Holdings (hereafter "Defendant" or "LabCorp"), to obtain declaratory, injunctive and monetary relief for a class of individuals against Defendant for its failure to safeguard its client's personal and private Protected Health Information ("PHI") including but not limited to medical information, names, health plan identification numbers, gender, health plan eligibility dates, insurance types, coverage information and physician information as well as Personal Identifying Information ("PII") including names, dates of birth, social security numbers, financial

information, and phone numbers, which Defendant collected from Plaintiff and Class Members (PII and PHI collectively referred to as "Private Information"), and for failing to provide timely, accurate and adequate notice to Plaintiff and other Class Members that their Private Information had been stolen and failing to provide timely, accurate and adequate notice of precisely what types of information were stolen.

2. On June 4, 2019, LabCorp announced, via a periodic public filing with the Securities and Exchange Commission ("SEC") that American Medical Collection Agency ("AMCA"), a vendor utilized by LabCorp for billing and collections, had failed to secure the information of LabCorp customers on its systems, resulting in a data breach which exposed the PII and PHI of up to 7.7 million LabCorp customers. (hereinafter referred to as "the Data Breach"). According to LabCorp, the PII/PHI that was exposed in the breach included customers' "first and last name, date of birth, address, phone, date of service, provider, and balance information. AMCA's affected system also included credit card or bank account information that was provided by the consumer to AMCA (for those who sought to pay their balance)." Further, according to LabCorp, the breach occurred between August 1, 2018 and March 30, 2019.[1]

3. On June 13, 2019, LabCorp provided additional information about the breach on its website.[2] That information indicated that:

- AMCA was an external collection agency used by LabCorp and other companies.
- LabCorp referred patient balances to AMCA when its direct collection efforts were unsuccessful.

[1] *See* June 4, 2019 SEC Form 8-K Filing, available at https://www.sec.gov/Archives/edgar/data/920148/000119312519165091/d757830d8k.htm (last accessed July 5, 2019).
[2] LabCorp, *Information about the AMCA Data Security Incident*, June 13, 2019, available at https://www.labcorp.com/AMCA-data-security-incident (last accessed July 5, 2019).

- According to AMCA, there was a security incident involving unauthorized activity on an AMCA information technology system between August 1, 2018 and March 30, 2019.

- AMCA's affected system contained information provided by LabCorp and patients.

- The website disclosure purported to state that the limited information provided by LabCorp to AMCA included patient personal information, but did not include test, laboratory results, or clinical information.

- Also, that the information on AMCA's affected system did not contain Social Security Numbers or insurance information for LabCorp patients.

- The disclosure stated that AMCA's affected system may have contained credit card or bank account information that patients provided to AMCA to make payments.

- LabCorp asserted that it had not yet been allowed to independently verify the information provided by AMCA about the AMCA incident. Our investigation is ongoing…

- It asserted that AMCA's System Did Not Include Healthcare Information or Social Security Numbers.

- It admitted that approximately 7.7 million patients had information on AMCA's affected system that was provided by LabCorp.

- It stated that LabCorp did not provide ordered test, laboratory results, or clinical information to AMCA.

- LabCorp asserted that AMCA had advised LabCorp that Social Security Numbers and insurance identification information are not stored or maintained for LabCorp patients.

- It disclosed that the information provided by LabCorp to AMCA could include first and last name, date of birth, address, phone, date of service, provider, and balance information.

- It disclosed that AMCA had indicated that its affected system also included credit card or bank account information that was provided to AMCA by approximately 200,000 patients when they made payments.

4. LabCorp failed to disclose the Data Breach for nearly two months from the time it was first discovered, further harming the customers whose information was included in the breach.

PARTIES

5. Plaintiff, Mohamad Mohamad, is an adult individual residing in Paterson, New Jersey who was notified by letter dated June 4, 2019 from AMCA that his PII/PHI was included in the breach. As a result of the Data Breach and LabCorp's failure to ensure his information was secure, Plaintiff will continue to be at heightened risk for medical fraud, financial fraud, and identity theft along with attendant damages for years to come. Further, as a result of the Data Breach, Mr. Mohamad has spent an additional five to ten hours monitoring his bank and credit card accounts for fraud, as recommended in the notification letter.

6. Defendant, Laboratory Corporation of America Holdings abbreviated herein as LabCorp is a Delaware company headquartered at 358 South Main Street, Burlington, North Carolina. It operates one of the largest clinical laboratory networks in the world, processing approximately 2.5 million lab tests weekly across 36 primary laboratories. It may be served with process at its Burlington NC address or c/o Registered Agent, 2626 Glenwood Avenue, Suite 550, Raleigh, NC 27608.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are approximately 7.7 million putative

class members, at least some of whom, including Plaintiff, have a different citizenship from Defendant.

8. This Court has jurisdiction over Defendant as LabCorp is headquartered and operates in this District.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

A. Defendant LabCorp and its Privacy Commitments to Consumers.

10. Defendant, LabCorp, is a global life sciences company which provides diagnostic, drug development and technology enabled solutions for more than 120 million patient encounters per year. LabCorp typically processes tests on more than 2.5 million patient specimens per week and supports clinical trial activity in approximately 100 countries through what it characterizes as its industry-leading central laboratory business.[3] Obviously, protecting patient and consumer private personal and health information is part of LabCorp's core business model and the company is fairly obligated to strictly safeguard such data and, to fully disclose and remedy any breach.

11. LabCorp recognizes that customers of its laboratory services value privacy, and therefore, on its website LabCorp maintains pages dedicated to the promises it makes to customers regarding the protection of their PII and PHI.

[3] LabCorp, *About Us*. Avaliable at https://www.labcorp.com/about-us (last accessed July 5, 2019).

12. With regard to PII, Defendant maintains a Website Privacy Policy, which provides[4]:

> Laboratory Corporation of America Holdings and its subsidiaries, including Laboratory Corporation of America (collectively "LabCorp"), is a national clinical laboratory that fully embraces genomic and molecular testing and has pioneered new diagnostic technologies. LabCorp is committed to protecting the privacy of every person who visits the LabCorp website so that each person will feel free to gather information, make inquiries/comments, and/or perform bill payment functions on our site. As part of LabCorp's effort to protect the privacy of your personal information while visiting the LabCorp site, we created this web privacy statement to inform you of the privacy standards used to ensure the security and confidentiality of your information. The following information details how LabCorp uses information that you provide to us via the LabCorp website and answers commonly asked questions regarding the privacy of your individual information….
>
> **Disclosure of Personal Information to Third Parties**
>
> We will not give, sell, rent, loan or otherwise disclose any personal information to any third party, unless (1) you have authorized us to do so, (2) we are legally required to do so, for example, in response to a subpoena, court order or other legal process, and/or (3) it is necessary to do so in order to protect and defend the rights or property of this website. **For example, with your consent, we may disclose your personal information to a third-party vendor that we engage to mail your test results to you. We contractually require such third-party vendors and contractors to comply with strict standards regarding security and confidentiality.**

(Emphasis added).

13. With regard to PHI, Defendant maintains a Notice of Privacy Practices on its website, which provides in relevant part[5]:

[4] LabCorp Web Privacy Policy. Available at https://www.labcorp.com/hipaa-privacy/web-privacy-policy (last accessed July 5, 2019)

> Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), LabCorp is required by law to maintain the privacy of health information that identifies you, called protected health information (PHI), and to provide you with notice of our legal duties and privacy practices regarding PHI. LabCorp is committed to the protection of your PHI and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation. We take this commitment seriously and will work with you to comply with your right to receive certain information under HIPAA…
>
> **Information Breach Notification**
>
> LabCorp is required to provide patient notification if it discovers a breach of unsecured PHI unless there is a demonstration, based on a risk assessment, that there is a low probability that the PHI has been compromised. You will be notified without unreasonable delay and no later than 60 days after discovery of the breach. Such notification will include information about what happened and what can be done to mitigate any harm.

14. LabCorp collects and stores PII and PHI which it provides to vendors and subcontractors like AMCA to maximize its profits. LabCorp has committed and represented to consumers that it would ensure such vendors and subcontractors maintained the security of information provided to them.

15. Consumers place value in data privacy and security, and they consider it when engaging services. Plaintiff and Class Members would not have utilized LabCorp's services had they known that Defendant did not take all necessary precautions to secure or ensure that its subcontractors and vendors secured the personal data given to them by consumers. Further, the value of such private data only magnifies as growth of the internet and e-commerce grows more significant.

[5] LabCorp Notice of Privacy Practices, https://www.labcorp.com/hipaa-privacy/hipaa-information, (last accessed July 5, 2019).

16. LabCorp failed to disclose its negligent and insufficient data security practices or those of its subcontractors and vendors. Consumers relied on and/or were misled by this omission into using Defendants' services.

B. Defendant was Aware that Thieves and Hackers Target the Medical Industry.

17. The technology and medical industry is rife with similar examples of hackers targeting users' Private Information, including the hacks of Anthem[6], Premera[7], and St. Joseph Health System[8] among others, all of which predate the time-frame LabCorp has identified regarding the Data Breach at issue in the present lawsuit.

18. LabCorp itself has been the subject of prior attacks by hackers, requiring the shutdown of certain parts of its network on July 18, 2018.[9]

19. As early as 2014 the FBI alerted healthcare firms that they were the target of hackers, stating "The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)".[10]

---

[6] Los Angeles Times, *Anthem is warning consumers about its huge data breach. Here's a translation*, March 6, 2015. Available at http://www.latimes.com/business/la-fi-mh-anthem-is-warning-consumers-20150306-column.html (last accessed July 5, 2019).

[7] New York Times, *Premera Blue Cross Says Data Breach Exposed Medical Data*, March 17, 2015. Available at http://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html?_r=0 (last accessed July 5, 2019).

[8] Napa Valley Register, *St. Joseph Health System sued for patient data breach*, April 9, 2012. Available at http://napavalleyregister.com/news/local/st-joseph-health-system-sued-for-patient-data-breach/article_948c0896-82a3-11e1-bed6-0019bb2963f4.html (last accessed July 5, 2019).

[9] Healthcare IT News, *LabCorp goes down after network breach, putting millions of patient records at risk*. July 17, 2018. Available at https://www.healthcareitnews.com/news/labcorp-goes-down-after-network-breach-putting-millions-patient-records-risk (last accessed July 5, 2019)

[10] Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014. Available at http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last accessed July 5, 2019).

Stolen Private Information Is Valuable to Hackers and Thieves.

20. It is well-known and the subject of many media reports that both Private Health Information and Personal Identifying Information are highly coveted categories of valuable information and a frequent target of hackers. This information is targeted not only for identity theft purposes, but also for committing healthcare fraud, obtaining medical services under another's insurance, as well as other nefarious uses, such as holding the data for ransom or selling it on the black market and the "dark web."

21. 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.[11] Despite well-publicized litigation and frequent public announcements of data breaches by medical and technology companies, LabCorp opted to maintain an insufficient and inadequate system to protect the PHI and PII of Plaintiff and Class Members and failed to properly ensure the vendors/subcontractors it provided PHI and/or PII to adequately secure such information.

22. Legitimate organizations and the criminal underground alike recognize the value of PII. Otherwise, they wouldn't aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million users, they also took registration data from 38 million users."[12] Similarly, in the Target (consumer retail chain) data breach, in addition to PCI data

[11] Elinor Mills, *Study: Medical identity theft is costly for victims*, March 3, 2010, 5:00am PST. Available at: https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed July 5, 2019).
[12]Verizon 2014 PCI Compliance Report, Available at http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last accessed July 5, 2019).

pertaining to 40,000 credit and debit cards, hackers stole PII pertaining to 70,000 users.

23. Biographical data is also highly sought after by data thieves. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts."[13] PII data has been stolen and sold by the criminal underground on many occasions, and the accounts of theft and unauthorized access have been the subject of many media reports. One form of identity theft, branded "synthetic identity theft," occurs when thieves create new identities by combining real and fake identifying information and then use those identities to open new accounts. As one expert stated: "This is where they'll take your Social Security number, my name and address, someone else's birthday and they will combine them into the equivalent of a bionic person. … It's tougher than even the toughest identity theft cases to deal with because they can't necessarily peg it to any one person."[14] In fact, the fraud might not be discovered until an account goes to collections and a collection agency researches the Social Security number.

24. Unfortunately, and as is alleged below, despite all of this publicly available knowledge of the continued compromises of Personal Identifying Information in the hands of third parties, such as health companies, Defendant's approach at maintaining the privacy of the Plaintiff's and the Class Members' PII and PHI was lackadaisical, cavalier, reckless, or at the very least negligent.

[13] Verizon Report, *supra*.
[14] Quotation from Adam Levin, Chairman of IDT911, which helps businesses recover from identity theft. Synthetic identity theft is harder to unravel than traditional identity theft.

C. This Data Breach Will Result in Additional Identity Theft and Identity Fraud.

25. During pertinent times, LabCorp failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII and PHI maintained on its systems and failed to ensure vendors/subcontractors entrusted with PII and PHI maintained reasonable security procedures and practices in light of the sensitive information provided by LabCorp to those third parties.

26. The ramifications of LabCorp's failure to keep or ensure that third parties kept Plaintiff's and Class Members' data secure are severe. As explained by the Federal Trade Commission:

> Medical identity theft happens when someone steals your personal information and uses it to commit health care fraud. Medical ID thieves may use your identity to get treatment — even surgery — or to bilk insurers by making fake claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits, and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[15]

27. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[16]

---

[15] Federal Trade Commission, *Medical ID Theft: Health Information for Older People*, available at https://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people (last accessed July 5, 2019).

[16] Federal Trade Commission, *Warning Signs of Identity Theft*, available at https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft last accessed July 5, 2019.

28. According to Javelin Strategy and Research, "1 in 4 notification recipients became a victim of identity fraud."[17]

29. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud standing on its own makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[18] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims."[19]

30. Javelin Strategy and Research reports that losses from identity theft increased to $21 billion in 2013.[20]

31. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("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.[21]

---

[17] See 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at www.javelinstrategy.com/brochure/276 last visited July 5, 2019 (the "2013 Identity Fraud Report").
[18] Victims of Identity Theft, 2012 (Dec. 2013) at 10, *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf, last accessed (July 5, 2019).
[19] *Id*. at 11.
[20] *See* 2013 Identity Fraud Report.
[21] GAO, Report to Congressional Requesters, at p.33 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (emphases added) (last visited Sept. 24, 2014).

32. Plaintiff and putative Class Members now face years of constant surveillance of their financial, personal and medical records. The Class is incurring and will continue to incur such damages in addition to any fraudulent charges made to their financial accounts or medical insurance, whether or not such charges are ultimately reimbursed by the credit card companies.

D. Defendant Failed to Maintain the Confidentiality of Plaintiff and Class Members' Private Health Information.

33. Defendant had a duty to maintain the confidentiality of Plaintiff and Class Members' PHI.

34. Defendant's duties included ensuring Plaintiff and Class Members' electronic protected health information was not made available or disclosed to unauthorized third persons or processes.

35. Defendant's duties also included protecting against reasonably anticipated threats or hazards to the security of Plaintiff and Class Members' Private Health Information

36. Defendant failed to adequately protect Plaintiff and Class Members' Private Health Information from the reasonably anticipated threat of hackers accessing LabCorp's systems or those of the vendors/subcontractors to whom LabCorp entrusted customer's PHI.

37. As a result of the Defendant's failure to protect against reasonably anticipated threats, the electronic PHI of Plaintiff and the Class was made available and disclosed to third persons.

38. Plaintiff and Class Members have a privacy right in their medical records and medical information.

39. As a result of Defendant's failure to maintain the confidentiality of Plaintiff and Class Members' Private Health Information, Plaintiff and Class Members suffered an injury through their loss of privacy, and through the unauthorized conversion, loss and theft of their personal and private electronic data which carries economic value and the compromise of which can harm credit reports and cause other loss.

E. Defendant's Conduct Violates HIPAA and Industry Standards.

40. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. § 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data that this Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

41. Defendant's breach resulted from a combination of insufficiencies that indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. LabCorp's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to adequately catalog the location of patients/customers', including Plaintiff's and Class Members', digital information;

d. Failing to properly encrypt Plaintiff's and Class Members' PII;

e. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to

allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. 164.312(a)(1);

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

h. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. 164.308(a)(6)(ii);

i. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. 164.306(a)(2);

j. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. 164.306(a)(4);

l. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. 164.502, *et seq.*;

m. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. 164.530(b) and 45 C.F.R. 164.308(a)(5); and

n. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. 164.530(c).

E. Plaintiff and Class Members Suffered Damages.

42. The Data Breach was a direct and proximate result of LabCorp's failure to properly safeguard and protect Plaintiff's and putative Class Members' Private Identifying Information and Private Health Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law. Defendant breached its duty including by LabCorp's failure to

establish and implement appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Personal Identifying Information and Personal Health Information to protect against reasonably foreseeable threats to the security or integrity of such information.

43. Plaintiff and Class Members' Personal Identifying Information and Private Health Information is private and sensitive in nature and was left inadequately protected by LabCorp. LabCorp did not obtain Plaintiff's and Class Members' consent to disclose either their Personal Identifying Information or their Private Health Information to any other person as required by applicable law and industry standards.

44. As a direct and proximate result of LabCorp's wrongful action and inaction and the resulting Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take time and effort to mitigate the actual and potential impact of the Data Breach on their lives by, among other things, placing "freezes" or "alerts" with credit reporting agencies, contacting their health insurance providers, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their medical "explanations of benefits" and credit reports and accounts for unauthorized activity.

45. Furthermore, Plaintiff and Class Members have suffered injuries in the loss of privacy through the disclosure of their Private Health Information.

46. LabCorp's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain or into criminal hands of Plaintiff and Class Members' Private Health Information and Personal Identifying

Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation including:

a. Theft of their personal, medical, and/or financial information;

b. Reputational harms suffered by Defendant's publication of private facts in the form of Plaintiff's and Class Members' medical records and related information;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal and medical information being placed in the hands of criminals;

d. The untimely and inadequate notification of the Data Breach;

e. The improper disclosure of Plaintiff's and Class Member's private information;

f. Loss of privacy;

g. Ascertainable loss in the form of out-of-pocket expenses and the value of their time and labor reasonably incurred to investigate, remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of their Personal Identifying Information and Private Health Information, for which there is a well-established national and international market and black market;

i. Overpayments to LabCorp for products and services in that a portion of the price paid for such products and services by Plaintiffs and Class Members to LabCorp was for the costs of reasonable and adequate safeguards and security measures that would protect users' Private Information, which LabCorp did not implement and, as a result, Plaintiffs and Class Members did not receive what they paid for and were overcharged by LabCorp; and

j. Damages caused by LabCorp continuing to inadequately secure Plaintiff's and Class Members' Personal Identifying Information and Private Health Information, as the evidence may show.

CLASS ACTION ALLEGATIONS

47. This action is brought and may properly proceed as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and LR

23.1. Plaintiff brings this action on behalf of himself and all others similarly situated. Plaintiff seeks certification of a Class, initially defined as follows:

> **All persons whose PII and/or PHI was exposed in the Data Breach announced on or about June 4, 2019.**

48. Plaintiff also seeks certification of a New Jersey Sub-Class, initially defined as follows:

> **All persons residing in the State of New Jersey whose PII and/or PHI was exposed in the Data Breach announced on July 5, 2019.**

49. The Class and Subclass for those whose benefit this action has been brought is so numerous that joinder of all members is impracticable, as Defendant has indicated it believes as many as 7.7 million individuals may have been impacted in the Data Breach.

50. All the individuals impacted by the breach had laboratory testing results disclosed to an unauthorized third party.

51. Plaintiff's claims are typical of the claims of the members of the Class, since all such claims arise out of Defendant's failure to safeguard or to ensure vendors/subcontractors safeguard users PII and PHI.

52. Plaintiff does not have interests antagonistic to the interests of the Class or Subclass.

53. The Class and Subclass, of which Plaintiff is a member, are readily identifiable by reference to Defendant's records.

54. Plaintiff will fairly and adequately protect the interests of the Class and Subclass and have retained competent counsel experienced in the prosecution of consumer litigation. Proposed Class Counsel has investigated and identified potential

claims in the action and has a great deal of experience in handling class actions, other complex litigation, and claims of the type asserted in this action.

55. There are common questions of law and fact effecting the rights of all class members, including the following:

a. Whether Defendant had a duty to protect patient PHI and/or PII;

b. Whether Defendant knew or should have known about its vendor/subcontractor's failure to adequately secure patient PHI and/or PII;

c. Whether Defendant violated common and statutory law by failing to promptly notify Class Members their Private Health Information and Personal Identifying Information had been compromised;

d. Whether Defendant was negligent in hiring an unqualified or improper third party to maintain patient PHI and/or PII.

e. Whether class members may obtain injunctive relief against Defendant to require that it safeguard or destroy, rather than retain as it has the Private Health Information and Personal Identifying Information of Plaintiff and the Class Members;

f. Whether Defendant continues to use inadequate security measures to secure Plaintiff and Class Members' Private Health Information and Personal Health Information;

g. Whether Plaintiff and Class Members are entitled to injunctive relief requiring LabCorp to improve the security measures utilized to secure Private Health Information and Personal Identifying Information.

h. Which security procedures and which data-breach notification procedure LabCorp should be required to implement as part of any injunctive relief ordered by the Court;

i. Whether LabCorp has contractual obligations to use reasonable security measures;

j. Whether LabCorp has complied with contractual obligations to use reasonable security measures and/or require third parties use reasonable security measures;

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

l. Whether LabCorp has implied contractual obligations to use reasonable security measures or require third parties entrusted with patient PHI and/or PII use adequate security measures;

m. Whether LabCorp has complied with implied contractual obligations to use reasonable security measures and or require third parties entrusted with patient PHI and/or PII use adequate security measures;

n. What security measures, if any, must be implemented by LabCorp to comply with its implied contractual obligations;

o. Whether LabCorp violated privacy laws in connection with the actions described here; and

p. What the nature of the relief should be, including equitable relief, to which Plaintiff and Class Members are entitled.

56. A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. While the economic damages suffered by the individual Class Members are significant, the amount is modest compared to the expense and burden of individual litigation. A class action will cause an orderly and expeditious administration of the claims of the Class and will foster economies of time, effort and expense.

57. The questions of law and/or fact common to the members of the Class predominate over any questions affecting only individual members.

58. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications, which would establish incompatible standards of conduct for the Defendant in this action or the prosecution of separate actions by individual members of the Class would create the risk that adjudications with respect to individual members of the Class and Subclass would as a practical matter be dispositive of the interests of the other members not parties to the

adjudications or substantially impair or impede their ability to protect their interests. Prosecution as a class action will eliminate the possibility of repetitious litigation.

59. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the class as a whole.

60. Plaintiff does not anticipate any difficulty in the management of this litigation.

COUNT ONE
Negligence
(On Behalf of Plaintiff and the Class)

61. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

62. Defendant, through the course of providing services to Plaintiff and the Class, required Plaintiff and Class members to provide PII and/or PHI.

63. Defendant knew, or should have known, of the risks inherent in collecting and storing the PII and PHI of Plaintiff and Class Members.

64. Plaintiff and the Class entrusted their PII and/or PHI to LabCorp with the understanding that LabCorp would ensure that such information would be safeguarded, both by LabCorp and by any vendors or subcontractors selected by LabCorp.

65. Upon accepting and storing Plaintiff's and Class Members' PHI and PII in their computer database systems, Defendant undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so. Further, Defendant had an obligation to ensure any vendor or subcontractor to whom Defendant supplied PHI and/or

PII for patients would utilize commercially reasonable methods to secure said information. LabCorp knew, acknowledged, and agreed that the Plaintiff and Class Member's PHI and PII was private and confidential and would be protected as private and confidential.

66. The breach of confidentiality for patient medical records, was a breach of the standard of care owed by Defendant to Plaintiff and Class Members.

67. Defendant breached its duties of care to Plaintiff and Class Members by failing to provide fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiffs' PHI and PII.

68. Defendant breached its duties of care to Plaintiff and Class Members by failing to ensure its vendors or subcontractors provided fair, reasonable or adequate computer systems and data security practices to safeguard Plaintiffs' PHI and PII.

69. Defendant acted with wanton disregard for the security of Plaintiff and Class Members' PHI and PII. Defendant knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the PHI and PII in health care databases such as LabCorp's and/or its vendors/subcontractors.

70. The law imposed an affirmative duty on LabCorp to timely discover and disclose the unauthorized access and theft of the PHI and PII to Plaintiffs and the Class so that Plaintiffs and Class Members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

71. To date, LabCorp has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access or the nature of the information it provided to its vendors/subcontractors which was breached and continues to breach its disclosure obligations to Plaintiff and the Class.

72. Defendant has not notified the Class of which medical records were disclosed, and specifically what PHI and Personal Identifying Information was disclosed for each Class Member in the breach.

73. Defendant also breached its duty to Plaintiff and the Class Members to adequately protect and safeguard Plaintiff and Class Members' information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, LabCorp failed to provide adequate supervision and oversight of the Private Information with which it is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiffs' and Class Members' Private Information, misuse the Private Information, and intentionally disclose it to others without consent.

74. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect Plaintiff and Class Members' Private Information from being foreseeably captured, accessed, disseminated, stolen, and misused, LabCorp unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff and Class Members' Private Information during the time it was within LabCorp's possession or control.

75. Further, through its failure to timely discover and provide clear

notification of the Data Breach to consumers, LabCorp prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their Private Information.

76. Upon information and belief, LabCorp improperly and inadequately safeguarded the Private Information of Plaintiff and Class Members in deviation from standard industry rules, regulations, and practices at the time of the Data Breach.

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

78. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Private Information; failing to conduct adequate regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and Class Members' Private Information; and failing to provide Plaintiffs and Class Members with timely and sufficient notice that their sensitive Private Information had been compromised.

79. Neither Plaintiff nor the other Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

80. As a direct and proximate cause of Defendant's conduct, Plaintiff and the Class suffered damages including, but not limited to: damages from identity theft, which may take months, if not years, to discover and detect, given the far-reaching, adverse, and detrimental consequences of identity theft and loss of privacy. The nature of other forms

of economic damage and injury may take years to detect and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT TWO
Negligent Hiring and Retention
(On Behalf of Plaintiff and the Class)

81. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

82. Defendant failed to exercise reasonable care in its hiring and retention practices to discover whether its third-party vendors and/or employees were unfit, incompetent, unable, or unwilling to employ adequate security measures for consumer's PII which would create a risk of harm to others in the capacity for which those third-party vendors and/or employees had been hired.

83. As a direct and proximate result of the aforesaid acts, omissions, negligence, carelessness and/or recklessness of the Defendant, the Plaintiff and the class was caused to suffer unlawful, extreme and unreasonable invasions of their privacy, economic harms and other damages including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses. Plaintiff and the subclass are entitled to damages under the act, including but not limited to actual damages for the disclosure, equitable relief in the form of appropriate notice advising them of the laboratory results disclosed, equitable relief in the

form of requiring Defendant to implement appropriate security measures to protect Plaintiff and Sub Class Members' records in the future, attorney's fees and costs and punitive damages.

COUNT THREE
Breach of Contract
(On Behalf of Plaintiff and the Class)

84. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

85. As set forth above, Plaintiff and Class Members who received laboratory services from Defendant and provided Defendant with their PHI/PII.

86. As set forth above, the contract between Plaintiff and Class members and LabCorp was supported by consideration in many forms including the payment of monies for laboratory testing services.

87. Plaintiff and Class Members performed pursuant to these contracts, and satisfied all conditions, covenants, obligations, and promises of the agreements.

88. Under the contracts, Defendant was obligated, as outlined in the Notice of Privacy Practices and Privacy Policy, to maintain the confidentiality of Plaintiff and Class Member's PHI and PII and to ensure any third-party to whom Defendant provided Class Member's PHI and PII ensured the confidentiality of that information.

89. Defendant and/or its vendor/subcontractor's failure to maintain the confidentiality of Plaintiff and Class Members Private Health Information was a breach of Defendant's contractual obligations as outlined in the Notice of Privacy Practices.

90. Defendant's failure to maintain the confidentiality of Plaintiff and Class Members' Personal Identifying Information was a breach of Defendant's contractual obligations as outlined in the Privacy Policy.

91. As a result of Defendant's breach of contract, by failing to adequately secure Plaintiff and Class Member's PHI and PII, Plaintiff and Class Members did not receive the full benefit of the bargain, and instead received services that were less valuable than described in the contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in value between what was promised and what LabCorp ultimately provided.

92. As a result of LabCorp's breach of contract, Plaintiff and Class Members have suffered actual damages resulting from the theft of their PHI and PII, and remain at imminent risk of suffering additional breaches in the future.

COUNT FOUR
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

93. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

94. LabCorp required Plaintiff and Class Members to provide PHI and PII to Defendant in order to receive laboratory testing, including names, addresses, dates of birth, social security numbers and financial information.

95. In providing their PHI and/or PII, Plaintiffs and Class Members entered into implied contracts with LabCorp pursuant to which LabCorp agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised. LabCorp further agreed that such

information would only be supplied to vendors/subcontractors who would also protect such information.

96. Each use of a LabCorp service or product made by Plaintiff and Class Members was made pursuant to the mutually agreed-upon implied contract with LabCorp under which LabCorp agreed to safeguard and protect Plaintiff's and Class Members' PHI and PII and to timely and accurately notify them if such information was compromised or stolen.

97. Plaintiff and Class Members would not have provided and entrusted their PHI and PII to LabCorp in the absence of the implied contract between them and LabCorp.

98. Plaintiff and Class Members fully performed their obligations under the implied contracts with LabCorp.

99. LabCorp breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect the PHI and PII of Plaintiff and Class Members and by failing to provide timely and accurate notice to them that their Private Information was compromised in and as a result of the Data Breach.

100. As a direct and proximate result of LabCorp's breaches of the implied contracts between LabCorp and Plaintiff and Class Members, Plaintiff and Class Members sustained actual losses and damages as described in detail above.

COUNT FIVE
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

101. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

102. Plaintiff and Class Members' PII and PHI is private information.

103. Dissemination and publication of Plaintiff and Class Members' PII/PHI would be offensive to a reasonable person.

104. The public has no legitimate interest in being apprised of Plaintiff and Class members' PII/PHI.

105. Defendant's failure to safeguard and protect Plaintiff and Class Members' PII/PHI directly and proximately resulted in unreasonable publicity to the private lives of Plaintiff and Class members.

106. Plaintiff and Class members have a legal interest in the privacy of their PII/PHI.

107. Defendant's failure to safeguard and protect Plaintiff and Class Member's PII/PHI was a direct and proximate cause of an unauthorized third party accessing and obtaining Plaintiff and Class Members' PII/PHI as a matter of law.

108. Defendant's failure to safeguard and protect Plaintiff and Class Members' PII/PHI deprived Plaintiff and Class Members of their legal interest in the privacy of that information, causing them damages.

109. As a result of Defendant's actions and inactions resulting in Plaintiff and Class Members loss of privacy, Plaintiff and Class Members were and continue to be injured and have suffered damages.

COUNT SIX
Publication of Private Facts
(On Behalf of Plaintiff and the Class)

110. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

111. Defendant, by and through its failure to adequately safeguard Plaintiff and Class Member's PHI and PII, made Plaintiff and Class Members' information public.

112. Plaintiff and Class Members' relevant information including the contents of private medical results, personal data, lists of treating doctors and other sensitive information was and is private information.

113. Dissemination of information such as the PHI and PII revealed by Defendant about Plaintiff and Class Members would be offensive to a reasonable person.

114. Plaintiff and other Class Member's PHI and PII is not of legitimate public concern, and there is no legitimate public interest in the public being apprised of said information.

115. Plaintiff and other Class Members did not consent to the disclosure of their PHI and PII.

116. As a result of Defendant' s actions and inactions resulting in Plaintiff and Class Members loss of privacy, Plaintiff and Class Members were and continue to be injured and have suffered damages. Additionally, Plaintiff and Class Members are entitled to presumed damages as a result of Defendant's publication of private facts.

COUNT SEVEN
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

117. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

118. In the alternative to the above plead claims, Plaintiff and the Class allege that they have no adequate remedy at law and bring this unjust enrichment claim.

119. Plaintiff and Class Members conferred a monetary benefit on Defendant LabCorp.

120. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class Members.

121. A significant part of the amounts paid to Defendant as a result of Plaintiff and Class Members' use of its services was to be used and should have been used by Defendant to secure and strictly protect private and personal data and to pay for the administrative costs of reasonable data privacy and security practices and procedures.

122. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages as aforesaid.

123. Under principals of equity, Defendant should not be permitted to retain the money it collected as a result of Plaintiff and Class Members' use of its services Defendant failed to implement, or to adequately implement, the data privacy and security practices and procedures that Plaintiff and Class Members were fairly entitled, and which were otherwise mandated by HIPAA regulations, federal, state and local laws, as well as industry standards.

124. LabCorp should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by LabCorp.

COUNT EIGHT

Violation of the New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-1, *et seq.*

(On Behalf of Plaintiff and the Sub-Class)

125. Plaintiff repeats and realleges all of the allegations set forth in the preceding paragraphs as if fully set forth herein.

126. Plaintiffs and the Class bring these claims against Defendant under the New Jersey Consumer Fraud Act.

127. Defendant sells "merchandise" as defined by the New Jersey Consumer Fraud Act by offering health services to the public.

128. Under applicable choice of law principles, the circumstances warrant application of New Jersey state substantive law.

129. Defendant engaged in unconscionable and deceptive acts and practices, misrepresentation and the concealment, suppression and omission of material facts with respect to the sale and advertisement of their services in violation of N.J.S.A. § 56:8-2, including by not limited to as follows:

a. Defendant misrepresented material facts pertaining to its services to consumers by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff and Class Members' PHI and PII from unauthorized disclosure, release, data breaches and theft;

b. It misrepresented material facts by representing to Plaintiff and Class members that Defendant did and would continue to comply with the relevant industry data security standards, state law and federal law with regard to the protection of Plaintiff and Class Members' PHI and PII;

c. Defendant knowingly omitted, suppressed and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff and the Class Members' PHI and PII with the intent that Plaintiff and the Class Members would rely on the omission, suppression and concealment;

d. Defendant engaged in unconscionable and deceptive acts and practices by failing to disclose the Data Breach to Plaintiff and Class Members in a timely and accurate manner in violation of N.J.S.A. § 56:8-163(a); and

e. Defendant misrepresented that it had fixed its security practices to stop continued intrusions, when in fact Defendant continues to be unaware, or unwilling to disclose, the facts of how the intrusion occurred originally.

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

131. Plaintiff and Class members are therefore entitled to injunctive relief, equitable relief, actual damages, treble damages, and attorneys' fees and costs pursuant to N.J.S.A. § 56:8-19.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests that the Court enter judgment in his favor and against LabCorp as follows:

a. For an Order certifying the Class as defined herein, and appointing Plaintiff and his Counsel to represent the Class as Class Counsel and as the Class Representative;

b. For equitable relief enjoining LabCorp from engaging in the wrongful conduct complained of here pertaining to the misuse and/or disclosure of Plaintiff and Class Members' Private Health Information and Personal Identifying Information, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiff and Class Members;

c. For equitable relief compelling LabCorp to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class Members the type of Private Health Information and Personal Identifying Information compromised;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of LabCorp's wrongful conduct;

e. For an award of actual damages and compensatory damages, in an amount to be determined;

f. For an award of treble damages, as allowable by law;

g. For an award of costs of suit and attorneys' fees, as allowable by law; and

h. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

Dated: July 16, 2019.

WALLACE & GRAHAM, P.A.

s/ William M. Graham, Esq.
William M. Graham, Esq., N.C. State Bar No. 17972
Mona Lisa Wallace, N.C. State Bar No. 9021
John Hughes, N.C. State Bar No. 22126
Wallace & Graham, P.A.
525 North Main Street
Salisbury, NC 28144
Phone: 704-633-5244
Fax: 704-633-9434
mwallace@wallacegraham.com
jhughes@wallacegraham.com
bgraham@wallacegraham.com

LOCKS LAW FIRM, LLC
James A. Barry, Esq.
801 N. Kings Highway
Cherry Hill, NJ 08034
jbarry@lockslaw.com
Tel: (856) 663-8200
Pending pro hac vice admission

THE KIM LAW FIRM, LLC
Yongmoon Kim, Esq.
411 Hackensack Ave, Suite 701
Hackensack, NJ 07601
ykim@kimlf.com
Tel: (201)273-7117
Pending pro hac vice admission

Attorneys for Plaintiff and the Putative Class