Exhibit C5

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA

DENISE BROWN-WELLS on behalf of herself and all others similarly situated, **Plaintiff** **v.** **LABORATORY CORPORATION OF AMERICA HOLDINGS,** **Defendant.**	**CASE NO.:** **CLASS ACTION** **COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORY AND INJUNCTIVE RELIEF** **DEMAND FOR JURY TRIAL**

Plaintiff Denise Brown-Wells ("Plaintiff"), individually and on behalf of those similarly situated, brings this class action lawsuit against Laboratory Corporation of America Holdings ("LabCorp") ("Defendant") based upon personal knowledge as to herself, and on information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendant for: failing to properly secure and safeguard protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), medical information, and other personally identifiable information (collectively, "PII")[1]; failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members (defined below) that the integrity of their PII had been compromised; and failing to provide timely, accurate,

[1] PII includes, but is not limited to, protected health information as defined by the Health Insurance Portability and Accountability Act, medical information, and other personally identifiable information including, without limitation to, names, health plan identification numbers, social security numbers, financial information, dates of birth, gender, address, health plan names, health plan eligibility dates, insurance types and coverage information.

and adequate notice to Plaintiff and other Class Members of the nature and scope of the PII that was exposed.

2. On June 4, 2019, LabCorp publicly announced that its billing collections vendor, AMCA, had been breached exposing the PII of as many as 7.7 million LabCorp customers whose data was stored on the affected system. LabCorp had provided its customer PII as part of its bill collection protocols. According to LabCorp, the PII consisted of customers "first and last name, date of birth, address, phone, date of service, provider, and balance information. [The][] 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)" ("Data Breach").[2] The Data Breach occurred between August 1, 2018 and March 30, 2019.

3. Despite the breadth and sensitivity of the PII that was exposed, and the attendant consequences to patients as a result thereof, LabCorp failed to disclose the Data Breach for nearly two months from the time it was first discovered, further exacerbating harm to patients. Moreover, to date, LabCorp has not disclosed the full extent and nature of the Data Breach, nor offered anything to its patients to address and compensate for the harm they have suffered.

4. This Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Patient PII.

5. Defendant disregarded the rights of Plaintiff and Class Members by: intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable

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

measures to ensure its data systems were protected against unauthorized intrusions; failing to follow reasonable practices in hiring third party vendors who would be responsible for PII; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Patient PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

6. As a result of Defendant's failure to implement and follow basic security procedures, patient PII is now in the hands of thieves. Plaintiff and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach and will forever be at a heightened risk of identity theft and fraud.

7. Plaintiff, on behalf of all others similarly situated, alleges claims for negligence, invasion of privacy, breach of contract, breach of implied contract, unjust enrichment, breach of fiduciary duty, breach of confidence and violation of Florida's Unfair and Deceptive Trade Practices Act and seeks to compel Defendant to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices to safeguard patient PII that remains in their custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

8. Plaintiff, Denise Brown-Wells is a resident of Fort Lauderdale, Florida and a LabCorp patient. On or about June 6, 2019, Ms. Wells received a "Notice of Data Breach" from AMCA indicating that her PII had been improperly exposed.

9. As a result of the Data Breach, and Defendant's failure to prevent it, Plaintiff will continue to be at heightened risk for medical fraud, financial fraud, and identity theft along with their attendant damages for years to come.

10. Defendant, Laboratory Corporation of America Holdings 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.

11. LabCorp maintains a web portal through which patients can interact with the company and provide a range of PII. The website provides a series of terms and conditions, which includes the following: "[t]he Online Services can be accessed from the United States and other countries worldwide. Since the laws of each State or country may differ, you agree that the statutes and laws of the State of North Carolina, without regard to any principles of conflicts of law, will apply to all matters relating to your access to or use of the Online Services."

JURISDICTION AND VENUE

12. 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 have a different citizenship from Defendant.

13. This Court has jurisdiction over Defendant as LabCorp is headquartered and operates in this District and Defendant, through its business operations intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

14. 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.

STATEMENT OF FACTS

A. *The Data Breach*

15. On June 4, 2019, LabCorp announced via a periodic public filing on Form 8-K that the highly sensitive PII of approximately 7.7 million of its patients had been improperly exposed over a seven-month period. The breach occurred on the system of LabCorp's billing collections vendor, AMCA. According to the filing, between August 1, 2018 and March 30, 2019 an unauthorized user gained access to AMCA's system which contained patient PII provided by LabCorp. According to LabCorp, the Data Breach exposed its 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)."[3] According to the June 4, 2019, public filing:

> In response to questions it has received, LabCorp® (NYSE: LH) announced that it has been notified by Retrieval-Masters Creditors Bureau, Inc. d/b/a American Medical Collection Agency (AMCA) about unauthorized activity on AMCA's web payment page (the AMCA Incident). According to AMCA, this activity occurred between August 1, 2018, and March 30, 2019. AMCA is an external collection agency used by LabCorp and other healthcare

[3] https://www.sec.gov/Archives/edgar/data/920148/000119312519165091/d757830d8k.htm (last visited June 23, 2019).

> companies. LabCorp has referred approximately 7.7 million consumers to AMCA whose data was stored in the affected AMCA system. AMCA's affected system included information provided by LabCorp. That information could include first and last name, date of birth, address, phone, date of service, provider, and balance information. AMCA's affected system also included credit card or bank account information that was provided by the consumer to AMCA (for those who sought to pay their balance). LabCorp provided no ordered test, laboratory results, or diagnostic information to AMCA. AMCA has advised LabCorp that Social Security Numbers and insurance identification information are not stored or maintained for LabCorp consumers.
>
> AMCA has informed LabCorp that it is in the process of sending notices to approximately 200,000 LabCorp consumers whose credit card or bank account information may have been accessed. AMCA has not yet provided LabCorp a list of the affected LabCorp consumers or more specific information about them.
>
> AMCA has indicated that it is continuing to investigate this incident and has taken steps to increase the security of its systems, processes, and data. LabCorp takes data security very seriously, including the security of data handled by vendors. AMCA has informed LabCorp that it intends to provide the approximately 200,000 affected LabCorp consumers with more specific information about the AMCA Incident, in addition to offering them identity protection and credit monitoring services for 24 months. LabCorp is 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.
>
> In response to initial notification of the AMCA Incident, LabCorp ceased sending new collection requests to AMCA and stopped AMCA from continuing to work on any pending collection requests involving LabCorp consumers.

Id.

16. On June 13, 2019, LabCorp provided, *inter alia*, the following additional information about the Data Beach.

- AMCA is an external collection agency used by LabCorp and other companies.
- LabCorp referred patient balances to AMCA when our direct collection efforts were unsuccessful.
- 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.
- Approximately 7.7 million patients had information on AMCA's affected system that was provided by LabCorp.
- Information provided by LabCorp to AMCA could include first and last name, date of birth, address, phone, date of service, provider, and balance information.
- AMCA has 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.
- AMCA has advised LabCorp that Social Security Numbers and insurance identification information are not stored or maintained for LabCorp patients.
- AMCA's affected system may have contained credit card or bank account information that patients provided to AMCA to make payments.
- LabCorp has not yet been allowed to independently verify the information provided by AMCA about the AMCA incident. Our investigation is ongoing.[4]

Steps Being Taken By AMCA

- AMCA has indicated that it is continuing to investigate this incident; that it has taken steps to increase the security of its systems, processes, and data; and that it has been in contact with law enforcement regarding the incident.
- AMCA has advised LabCorp that AMCA intends to provide more specific information to approximately 200,000 LabCorp patients who had certain financial information in AMCA's affected system.
- AMCA has indicated that it will offer identity protection and credit monitoring services for 24 months to those patients it notifies about this incident.

LabCorp Takes Data Security Very Seriously

[4] https://www.labcorp.com/AMCA-data-security-incident (last visited June 23, 2019).

- LabCorp takes data privacy and security very seriously, including the security of data handled by vendors.
- LabCorp has made and will continue to make significant investments to enhance the security of its information technology and data systems.

17. While LabCorp stated that Social Security Numbers and insurance identification information were not "stored or maintained" for LabCorp patients, they pointedly did not deny that such information had been transmitted to AMCA (and potentially could have been exposed). Moreover, while the PII of approximately 7.7 million LabCorp patients had been exposed, AMCA was limiting its response to only 200,000 of them. Despite an obligation to so, LabCorp has taken no steps to address the effects of the Data Breach with respect to its other 7.5 million additional patients, nor to ensure that AMCA's "more specific information" provided to some 200,000 patients was meaningful and appropriate.

18. Notwithstanding its claim to "take[] data privacy and security very seriously," LabCorp has done nothing to mitigate the harm to its 7.7 million patients, and instead just relied on the inadequate and paltry efforts of AMCA.

B. Defendant's Privacy Practices

19. LabCorp maintains a series of privacy policies which discuss LabCorp's commitments regarding the protection of consumers' PII and PHI. The policies are contained in its Website Privacy and HIPAA Information policies which state in relevant part:

Website Privacy Policy[5]

[5] https://www.labcorp.com/hipaa-privacy/web-privacy-policy

LabCorp is committed to protecting the privacy of every person who visits the LabCorp Web site 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.

HIPAA Information[6]

LabCorp's Notice of Privacy Practices

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

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

[6] https://www.labcorp.com/hipaa-privacy/hipaa-information

include information about what happened and what can be done to mitigate any harm.

20. LabCorp collects and stores an enormous amount of PII which it provides to its vendors and sub-contractors such as AMCA to further its business. As recipients of sensitive patient PII, AMCA is similarly obligated to safeguard the integrity of such data on behalf of LabCorp patients.

21. Indeed, AMCA boldly states that they are "compliant with all Federal and State Laws and are members of ACA International. We provide our services adhering to the ethical guidelines expected from a National Accounts Receivable Management firm."[7]

22. 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 the personal data given to them by consumers.

23. Defendant failed to disclose their negligent and insufficient data security practices, and those of its subcontractors. Consumers relied on, or otherwise were misled by this omission, in deciding to use Defendant's services.

C. Defendant Was Aware That the Medical Industry was a Favorite Target of Hackers

[7] Available at http://amcaonline.com/about.php (last visited June 5, 2019)

24. The technology and medical industry are rife with similar examples of hackers targeting users' Private Information, including Anthem[8], Premera[9], and St. Joseph Health System[10] among others, all of which predate the time-frame Defendant have identified regarding the Data Breach at issue in the present lawsuit. In fact, LabCorp itself was targeted by hackers and its customer data held ransom less than a year ago.[11]

25. Indeed, as early as 2014, the FBI alerted healthcare stakeholders that they were the target of hackers, stating "[t]he 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)."[12] Defendant's failure to heed this warning and to otherwise maintain adequate security practices resulted in this Data Breach.

D. The Value of Personally Identifiable Information

---

[8] 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 December 19, 2016.

[9] 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 December 19, 2016.

[10] 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 December 19, 2012.

[11] https://www.bankinfosecurity.com/labcorp-still-recovering-from-ransomware-attack-a-11235, last accessed June 23, 2019.

[12] 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 December 19, 2016.

26. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[13] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[14] The FTC acknowledges that identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[15]

27. PII is such a valuable commodity that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[16] Indeed, as a result of large-scale data breaches, Social Security numbers, healthcare information, and other PII have been made publicly available to identity thieves and cyber criminals.

28. Professionals tasked with trying to stop fraud and other misuse acknowledge that PII has real monetary value in part because criminals continue their efforts to obtain this data.[17] According to the Identity Theft Resource Center, 2017 saw 1,579 data breaches, representing a 44.7 percent increase over the record high figures

---

[13] 17 C.F.R § 248.201 (2013).

[14] *Id.*

[15] *Guide for Assisting Identity Theft Victims*, FTC (Sep. 2013), *available at*: https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (the "FTC Guide")(last visited April 21, 2019).

[16] FTC Guide, *supra* n.9.

[17] *Data Breaches Rise as Cybercriminals Continue to Outwit IT, CIO Magazine*, https://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html (last visited January 23, 2019).

reported a year earlier.[18] The Healthcare sector had the second largest number of breaches among all measured sectors and the highest rate of exposure per breach.[19]

29. Healthcare related data is among the most sensitive, and personally consequential when compromised. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident…came to about $20,000," and that the victims were forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage. [20] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.[21]

30. Defendant knew the importance of safeguarding patient PII entrusted to them, and of the foreseeable consequences if their data security systems were breached, including the significant costs that would be imposed on affected patients as a result of a breach.

E. Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII

---

[18] *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches, (last visited January 23, 2019).

[19] Identity Theft Resource Center, 2018 End -of-Year Data Breach Report. Available at https://www.idtheftcenter.org/2018-data-breaches/ (last visited April 19, 2019).

[20] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010) https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited April 21, 2019)

[21] *Id.*

31. Defendant acquires, collects, stores, and maintains a massive amount of protected health related information and other personally identifiable information on their patients.

32. As a condition of engaging in health services, LabCorp requires that their customers entrust them with highly sensitive personal information.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the Class Members' PII, LabCorp along with its vendors and sub-contractors assumed legal and equitable duties to those individuals and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' PII from disclosure.

34. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members, as current and former patients, relied on the Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

35. Defendant acknowledges, as they must, its obligation to maintain the privacy of patient PII entrusted to them. (e.g. "LabCorp takes data privacy and security very seriously, including the security of data handled by vendors").[22]

F. Defendant's Conduct Violates HIPAA and Industry Standard Practices

36. 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 Defendant left unguarded. The

[22] https://www.labcorp.com/AMCA-data-security-incident

HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

37. 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 CFR 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 CFR 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 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 CFR 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 CFR 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 CFR 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 CFR 164.306(a)(94);

l. Impermissibly and improperly using and disclosing protected health

information that is and remains accessible to unauthorized persons in violation of 45 CFR 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 CFR 164.530(b) and 45 CFR 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 CFR 164.530(c).

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

38. Defendant had a duty to maintain the confidentiality of Plaintiff and Class Members' PII.

39. Defendant's duties included ensuring Plaintiff's and Class Members' electronically protected PII was not made available or disclosed to unauthorized third persons or processes.

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

41. Defendant failed to adequately protect Plaintiff's and Class Members' PII from the reasonably anticipated threat of hackers accessing their systems and the PII contained therein.

42. As a result of the Defendant's failure to protect against reasonably anticipated threats, Plaintiff and the Class Members PII was improperly made available and disclosed to third persons.

43. Plaintiff and Class Members have a privacy right in their medical records, medical information, financial information and other PII.

44. As a result of Defendant's failure to maintain the confidentiality of Plaintiff and Class Members' PII, Plaintiff and Class Members suffered an injury through their loss of privacy.

H. Plaintiff and Class Members Suffered Damages

45. The ramifications of Defendant's failure to keep Patients' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

46. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

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

48. Defendant had the resources necessary to prevent the Breach, but neglected to adequately invest in data security measures, despite their obligations to protect patient data.

49. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into their systems and, ultimately, the theft of PII.

50. As a direct and proximate result of Defendant's wrongful actions and inaction, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[23]

51. Despite professing to "taking this matter very seriously" and being "committed to the privacy and security of [] patients' personal information," LabCorp have not offered patients anything to address the harm caused by them.

52. As a result of the Defendant's failure to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

[23] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited April 19,2019).

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. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

e. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in their possession; and

f. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

g. 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;

h. Overpayments for products and services in that a portion of the price paid for such products and services by Plaintiff and Class Members was for the costs of reasonable and adequate safeguards and security measures that would protect users' Private Information, which

Defendant did not implement and, as a result, Plaintiff and Class Members did not receive what they paid for and were overcharged.

53. In addition to a remedy for the economic harm, Plaintiff and the Class maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

54. Plaintiff seeks relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons whose PII was exposed to unauthorized third parties as a result of the Data Breach announced on June 4, 2019 ("Class").[24]

55. Plaintiff also seeks certification of a Florida Sub-Class defined as follows:

> All persons who reside in the State of Florida whose PII was exposed to unauthorized third parties as a result of the Data Breach announced on June 4, 2019 ("Florida Class").

56. Excluded from the Classes is Defendant and any of its affiliates, parents or subsidiaries; all persons who make a timely election to be excluded from the Class; government entities; and the judges to whom this case is assigned, their immediate families, and court staff.

57. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

---

[24] PII includes, but is not limited to, protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), medical information, and other personally identifiable information including, without limitation to, names, health plan identification numbers, dates of birth, gender, address, health plan names, health plan eligibility dates, insurance types and coverage information.

58. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

59. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of patients affected in the Data Breach is unknown, upon information and belief, it is approximately 7.7 million, and therefore meets the numerosity requirement of 23(a)(1).

60. **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. Common questions include:

a. Whether Defendant had a duty to protect patient PII;
b. Whether Defendant knew or should have known of the susceptibility of its, and its subcontractor's systems to a data breach;
c. Whether Defendant's security measures to protect their systems were reasonable in light of the FTC data security recommendations, and best practices recommended by data security experts;
d. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;
e. Whether Defendant's failure to implement adequate data security measures allowed the breach of its data systems to occur;
f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unlawful exposure of the Plaintiff's and Class Members' PII;

g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Defendant's failure to reasonably protect its systems and data network; and,

h. Whether Plaintiff and Class Members are entitled to relief.

61. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff is a patient whose PII was exposed in the Data Breach. Plaintiff's damages and injuries are akin to other Class members, and Plaintiff seeks relief consistent with the relief sought by the Class.

62. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representatives of the Class because Plaintiff is a member of the Classes she seeks to represent; are committed to pursuing this matter against Defendant to obtain relief for the Class; and have no conflict of interest with the Class. Moreover, Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation of this kind. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

63. **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. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to an individual Plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff 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.

64. **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.

65. 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 failed to timely notify the public of the Data Breach;
b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
c. Whether Defendant's security measures to protect its data systems were reasonable in light of FTC data security recommendations, and other best practices recommended by data security experts;
d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
e. Whether Defendant failed to take commercially reasonable steps to safeguard patient PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

66. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to patient names and addresses affected by the Data Breach. Using this information, Class members can be identified and ascertained for the purpose of providing notice.

FIRST CUASE OF ACTION
NEGLIGENCE
(AS TO DEFENDANT)

67. Plaintiff restates and realleges paragraphs 1 through 66 above as if fully set forth herein.

68. As a condition of receiving services, Plaintiff and Class Members were obligated to provide Defendant with their PII.

69. Plaintiff and the Class Members entrusted their PII to LabCorp with the understanding that LabCorp and its vendors and sub-contractors would safeguard their information.

70. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

71. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing the Defendant's security protocols to ensure that Plaintiff's and Class Members' information in its possession was adequately secured and protected and

that employees tasked with maintaining such information were adequately training on cyber security measures regarding the security of patient information.

72. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, the current cyber scams being perpetrated and that it had inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiff and the Class.

73. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decision not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiff and Class Members.

74. Plaintiff and the Class Members had no ability to protect their PII that was in Defendants' possession.

75. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

76. Defendant had a duty to have proper procedures in place to prevent the unauthorized dissemination of Plaintiff's and Class Members' PII.

77. Defendant has admitted that Plaintiff's and Class Members' PII was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

78. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting

and safeguarding the Plaintiff's and Class Members' PII while it was within the LabCorp's possession or control.

79. Defendant improperly and inadequately safeguarded Plaintiff's and Class Members' PII in deviation of standard industry rules, regulations and practices at the time of the Data Breach.

80. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' PII.

81. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiff and Class Members the existence, and scope of the Data Breach.

82. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII would not have been compromised.

83. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII of current and former patients and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class.

84. As a result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury 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.

SECOND CAUSE OF ACTION
NEGLIGENT HIRING AND RETENTION
(AS TO DEFENDANT)

85. Plaintiff restates and realleges paragraphs 1 through 84 above as if fully set forth herein.

86. Defendant failed to exercise reasonable care in its hiring and retention practices to discover whether their 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.

87. As a direct and proximate result of the aforesaid acts, omissions, negligence, carelessness and/or recklessness of the defendants, or some or any of them, Plaintiff and the Class were 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.

THIRD CAUSE OF ACTION
INVASION OF PRIVACY
(AS TO DEFENDANT)

88. Plaintiff restates and realleges paragraphs 1 through 87 above as if fully set forth herein.

89. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

90. Defendant owed a duty to patients, including Plaintiff and Class Members, to keep their PII contained as a part thereof, confidential.

91. Defendant failed to protect patient PII by allowing unauthorized third parties to gain unfettered access to Plaintiff's and Class Members' PII.

92. The unauthorized release of PII, especially the type related to personal health information, is highly offensive to a reasonable person.

93. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as part of their use of LabCorp's services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

94. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

95. Defendant acted with a knowing state of mind when they permitted the Data Breach because they were with actual knowledge that their information security practices were inadequate and insufficient.

96. Because Defendant acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

97. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' PII was disclosed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

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

FOURTH CAUSE OF ACTION
BREACH OF CONTRACT
(AS TO DEFENDANT)

99. Plaintiff restates and realleges paragraphs 1 through 98 above as if fully set forth herein.

100. Plaintiff and Class Members received medical services from Defendant LabCorp, and in so doing provided their PII.

101. The contract for these services as between Plaintiff and Class Members and LabCorp was supported by consideration in many forms including the payment of monies for medical services (e.g. laboratory testing services).

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

103. Under these contracts, Defendant LabCorp was obligated, as outlined in the Notice of Privacy Practices and Privacy Policy, to maintain the confidentiality of Plaintiff's and Class Member's PII.

104. LabCorp's failure to maintain the confidentiality of Plaintiff and Class Members PII was a breach of LabCorp's contractual obligations as outlined in their privacy practices.

105. By failing to adequately secure Plaintiff and Class Member's 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.

106. 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.

FIFTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(AS TO DEFENDANT)

107. Plaintiff restates and realleges paragraphs 1 through 106 above as if fully set forth herein.

108. Plaintiff and Class Members were required to provide their PII, including names, addresses, dates of birth, social security numbers, credit card and bank information, among other related information to Defendant as a condition of their use and or as a result of using and paying for LabCorp's services.

109. Plaintiff and Class Members paid money to Defendant in exchange for services, implicit in which were Defendant's promises to protect patient PII from unauthorized disclosure.

110. In their written privacy policies, Defendant promised Plaintiff and Class Members that they would only disclose protected health information and other PII under

certain circumstances, none of which relate to the Data Breach, and would otherwise comply with applicable state and federal laws.

111. Defendant promised and was otherwise obligated to comply with HIPAA standards and to make sure that Plaintiff's and Class Members' protected health information and other PII would remain protected.

112. Implicit in the agreement between the Defendant's patients, including Plaintiff and Class Members, to provide protected health information and other PII, and Defendant's acceptance of such protected health information and other PII, was Defendant's obligation to use the PII of patients for business purposes only, take reasonable steps to secure and safeguard that protected health information and other PII, and not make unauthorized disclosures of the protected health information and other PII to unauthorized third parties.

113. Further, implicit in the agreement, Defendant was obligated to provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their protected health information and other PII.

114. Without such implied contracts, Plaintiff and Class Members would not have provided their protected health information and other PII to Defendant.

115. Defendant had an implied duty to reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses.

116. Additionally, Defendant implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

117. Plaintiff and Class Members fully performed their obligations under the implied contract with Defendants, however, Defendant did not.

118. Defendant breached the implied contracts with Plaintiff and Class Members by:

a. failing to reasonably safeguard and protect Plaintiff and Class Members' PII, which was compromised as a result of the Data Breach;

b. failing to comply with their obligations to abide by HIPAA;

c. failing to ensure the confidentiality and integrity of electronic protected health information Defendants created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1);

d. 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 CFR 164.312(a)(1);

e. failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. 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 CFR 164.308(a)(6)(ii); and

g. failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

SIXTH CAUSE OF ACTION
UNJUST ENRICHMENT
(AS TO DEFENDANT)

119. Plaintiff restates and realleges paragraphs 1 through 118 above as if fully set forth herein.

120. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased medical services from Defendant and in so doing provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and have their PII protected with adequate data security.

121. Defendant knew that Plaintiff and Class Members conferred a benefit on Defendant and accepted and have accepted or retained that benefit. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

122. The amounts Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's network and the administrative costs of data management and security.

123. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

124. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

125. Defendant acquired the PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

126. If Plaintiff and Class Members knew that Defendant would not secure their PII using adequate security measures, they would not have engaged in transactions with Defendant.

127. Plaintiff and Class Members have no adequate remedy at law.

128. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant's fails to undertake appropriate and adequate measures to protect the PII of patients and in their continued possession; (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (viii) the diminished value of Defendant's services they received.

129. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

130. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

SEVENTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(AS TO DEFENDANT)

131. Plaintiff restate and reallege paragraphs 1 through 130 above as if fully set forth herein.

132. In light of the special relationship between Defendant and their Patients, whereby Defendant became guardians of Plaintiff's and Class Members' highly sensitive, confidential, personal, financial information, and other PII, Defendant became fiduciaries created by its undertaking and guardianship of the PII, to act primarily for the benefit of its Patients, including Plaintiff and Class Members, for: 1) the safeguarding of Plaintiff and Class Members' PII; 2) timely notify Plaintiff and Class Members' of a data breach or disclosure; and 3) maintain complete and accurate records of what and where Defendant's patients' information was and is stored.

133. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their patients' relationship, in particular to keep secure the PII of their patients.

134. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently investigate the Data Breach to determine the number of Class Members affected in a reasonable and practicable period of time.

135. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' protected health information and other PII.

136. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

137. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

138. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

139. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

140. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by 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 CFR 164.308(a)(6)(ii).

141. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

142. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

143. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by their workforce in violation of 45 CFR 164.306(a)(94).

144. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, et seq.

145. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b) and 45 CFR 164.308(a)(5).

146. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

147. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

148. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort

expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Patient PII in their continued possession; (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (viii) the diminished value of Defendant's services they received.

149. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

EIGHTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(AS TO DEFENDANT)

150. Plaintiff restates and realleges paragraphs 1 through 149 above as if fully set forth herein.

151. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' protected health information and other PII that Plaintiff and Class Members provided to Defendant.

152. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff's and Class Members' protected health information and other PII would be collected, stored, and protected in confidence, and would not be disclosed the unauthorized third parties.

153. Plaintiff and Class Members provided their respective protected health information and PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the protected health information and other PII to be disseminated to any unauthorized parties.

154. Plaintiff and Class Members also provided their respective protected health information and PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that protected health information and other PII from unauthorized disclosure, such as following basic principles of encryption and information security practices.

155. Defendant voluntarily received in confidence Plaintiff's and Class Members' protected health information and other PII with the understanding that protected health information and other PII would not be disclosed or disseminated to the public or any unauthorized third parties.

156. Due to Defendant's failure to prevent, detect, avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class Members' protected health information and other PII, Plaintiff's and Class Members' protected health information and PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

157. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

158. But for Defendant's disclosure of Plaintiff's and Class Members' protected health information and other PII in violation of the parties' understanding of confidence, their protected health information and other PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data

Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' protected health information and other PII, as well as the resulting damages.

159. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' protected health information and other PII. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' protected health information and other PII had numerous security vulnerabilities because Defendant failed to observe even basic security practices necessary to prevent fraudulent provider accounts from being created.

160. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Patient PII in their continued possession; (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (viii) the diminished value of Defendant's services they received.

161. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

NINTH CAUASE OF ACTION
VIOLATIONS OF THE OF THE FLORIDA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT, FLA. STAT. §§ 501.201, *et seq.*
(ON BEHALF OF THE FLORIDA CLASS ONLY)

162. Plaintiff restates and realleges Paragraphs 1 through 161 as if fully set forth here.

163. Plaintiff and Florida Class members are consumers within the meaning of Fla. Stat. § 501.203(7) (2006).

164. Defendant operating in Florida engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1). This includes but is not limited to the following:

a. Failing to enact adequate privacy and security measures to protect Florida Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Knowingly and fraudulently misrepresenting that they would maintain adequate data privacy and security practices and procedures to safeguard Florida Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

d. Knowingly omitting, suppressing, and concealing the inadequacy of their privacy and security protections for Florida Subclass Members' Personal Information;

e. Knowingly and fraudulently misrepresenting that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Florida Subclass Members' Personal Information, including but not limited to duties imposed by HIPAA and Fla. Stat. § 501.171(2);

f. Failing to maintain the privacy and security of Florida Subclass Members' Personal Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the foregoing paragraph, which was a direct and proximate cause of the Data Breach; and

g. Failing to disclose the Data Breach to Florida Subclass Members in a timely and accurate manner, in violation of Fla. Stat. § 501.171(4).

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

166. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Florida Subclass Members' Personal Information and that the risk of a data breach or theft was high. LabCorp's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Florida Subclass Members.

167. As a direct and proximate result of Defendant's violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff and Florida Class members suffered damages including, but not limited to damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by closely reviewing and monitoring their medical transactions for unauthorized activity, filing police reports, and 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.

168. Plaintiff and Florida Subclass Members seek actual damages under Fla. Stat. § 501.211(2), and attorneys' fees under Fla. Stat. § 501.2105(1), to be proven at trial.

169. Plaintiff and Florida Subclass Members also seek an order enjoining Defendant's unfair, unlawful, and/or deceptive practices, declaratory relief, and any other just and proper relief available under the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, et seq.

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, respectfully request the following relief:

a. An Order certifying this case as a class action;
b. An Order appointing Plaintiff as the class representative;
c. An Order appointing undersigned counsel as class counsel;
d. A mandatory injunction directing the Defendant to hereinafter adequately safeguard the Class' PII by implementing improved security procedures and measures;

e. An award of damages;

f. An award of costs and expenses;

g. An award of attorneys' fees; and

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

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial as to all issues so triable by a jury.

Dated: June 24, 2019

/s/ *Jean S. Martin*
Jean S. Martin
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
2018 Eastwood Road, Ste. 225
Wilmington, NC 28403
Tel: (813) 559-4908
Fax: (813) 222-4795
Email: jeanmartin@forthepeople.com

/s/ *John A. Yanchunis*
John A. Yanchunis
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel: (813) 223-5505
Email: jyanchunis@forthepeople.com