UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
GREENSBORO DIVISION

TATYANA SHULMAN, individually and on behalf of all those similarly situated, Plaintiff, v. LABORATORY CORPORATION OF AMERICA HOLDINGS, Defendant.	Civil Action No. 1:19-cv-616 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Tatyana Shulman ("Plaintiff"), individually and on behalf of a Class of similarly situated individuals (the "Class"), brings this Class Action Complaint against Defendant Laboratory Corporation of America Holdings ("LabCorp" or "Defendant"). Plaintiff alleges as follows upon personal knowledge as to her own acts and experience, and upon information and belief and the investigation of their attorneys as to all other matters:

NATURE OF THE CASE

1. Plaintiff bring this class action lawsuit on her behalf, and on behalf of a Class of similarly situated individuals, against Defendant for its failure to protect the confidential information of millions of consumers—including Personally Identifiable Information ("PII"), first and last names, dates of birth, addresses, telephone numbers, social security numbers, dates of service, Protected Health Information ("PHI"), provider names, payment balance information, credit cards or bank account information, and other confidential information (collectively, "Sensitive Information").

2. On June 4, 2019, LabCorp publicly announced that its customers' Sensitive Information was subject to unauthorized access by third parties between August 1, 2018 and March 30, 2019 due to a data security breach (the "Data Breach") of its billing collections

vendor, Retrieval-Masters Creditor's Bureau, Inc., d/b/a American Medical Collection Agency ("AMCA").

3. On or around May 14, 2019, AMCA notified LabCorp that there was a Data Breach of AMCA's web payment page. According to AMCA, the Data Breach began on August 1, 2018, and thereafter went undetected until March 30, 2019. After discovering the Data Breach, AMCA waited months before notifying affected individuals, preventing Plaintiff and the proposed Class from taking steps to prevent the further actual and potential misuse of their Sensitive Information.

4. AMCA's affected systems contained LabCorp's customers' Sensitive Information.

5. As of May 31, 2019, AMCA believed that the Data Breach affected the Sensitive Information of 7.7 million LabCorp customers.

6. At all relevant times, LabCorp promised and agreed —throughout its Notice of Privacy Practices and other written assurances—to safeguard and protect Sensitive Information in accordance with Health Insurance Portability and Accountability Act ("HIPAA") regulations, federal, state and local laws, and industry standards. In addition, LabCorp promised and agreed that its contracted service providers and other business associates, such as billing services providers, are "required to maintain the privacy" and security of PHI.[1]

7. Plaintiff and the Class would not have provided their Sensitive Information to Defendant, if Plaintiff and Class members knew that Defendant would breach its promises and agreements by failing to ensure that its vendors used adequate security measures and also by

[1] HIPAA Information, LabCorp, https://www.labcorp.com/hipaa-privacy/hipaa-information (last visited June 14, 2019).

providing customers' Sensitive Information to business associates that utilized inadequate security measures.

8. Defendant's failure to ensure that its vendors implement adequate security protocols compromised the Sensitive Information of millions of consumers, including Plaintiff and the Class, fell well short of Defendant's agreements and obligations, and also fell short of Plaintiff's and other Class members' reasonable expectations for protection of the Sensitive Information provided to LabCorp.

9. As a result of Defendant's conduct and the ensuing Data Breach, Plaintiff and the members of the proposed Class have suffered actual damages, and are at imminent risk of future harm, including identity theft and fraud which could result in further monetary loss. Accordingly, Plaintiff brings suit, on behalf of herself and Class of all others similarly situated, to seek redress for Defendant's unlawful conduct.

PARTIES

A. Plaintiff Tatyana Shulman

10. Plaintiff Tatyana Shulman is a citizen and resident of the State of Massachusetts.

11. Plaintiff Shulman went to a LabCorp laboratory to obtain medically prescribed blood testing in or around 2015.

12. Plaintiff Shulman provided LabCorp with Sensitive Information, including medical information and PII, as well as credit card information, as part of obtaining laboratory testing services from LabCorp.

13. After being billed for services, LabCorp sent Ms. Shulman's bill to AMCA for collections.

14. Upon information and belief, Plaintiff Shulman's Sensitive Information, including PII and financial information, was compromised in the Data Breach of LabCorp's billing service provider, AMCA.

15. Ms. Shulman experienced credit card fraud on two separate credit card accounts around the time the Data Breach. On or around May 24, 2019, two fraudulent international charges from Brazil appeared on one of Ms. Shulman's credit cards. This was the first time Ms. Shulman ever experienced fraudulent activity on this credit card account. Ms. Shulman had to spend time dealing with the credit card company to address the fraud and close the account. On or around June 14, 2019, fraudulent charges appeared on another one of Ms. Shulman's credit cards.

B. Defendant Laboratory Corporation of America Holdings

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

17. LabCorp processes millions of blood, urine and other diagnostic tests each week. It is one of the world's largest domestic commercial lab-testing companies and maintains a database containing health information on roughly half the U.S. population.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2) because (a) at least one member of the putative Class is a citizen of a state different from at least one Defendant, and (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

19. This Court has personal jurisdiction over Defendant because it is registered to and regularly does conduct business in this District, and a substantial part of the conduct alleged in this Complaint occurred in, was directed to, and/or emanated, in part, from this District.

20. Venue is proper pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the conduct alleged in this Complaint occurred in, were directed to, and/or emanated from this District. Venue is additionally proper because Defendant resides in this District, where its principal place of business is located.

FACTUAL BACKGROUND

A. LabCorp obtained Sensitive Information from Plaintiff and Class Members and Shared that Information with AMCA.

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

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

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

[3] *Id.* at 9.

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

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

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

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

---

[4] *Id.*

[5] *Id.*

[6] *Id.* at 5.

[7] *Id.* at 8.

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

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

26. LabCorp charges for the laboratory services it provides to patients, including Plaintiff Shulman and the putative Class. If the patient does not have insurance, or if the insurance does not cover the clinical laboratory testing services, the patient is responsible for paying for the services performed.[10]

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

28. LabCorp will refer unpaid bills to a collection agency. AMCA is an external collection agency utilized by LabCorp to collect unpaid bills. LabCorp has referred approximately 7.7 million patients, including Plaintiff Shulman and the putative Class, to AMCA. These patients' data was stored in the AMCA systems that were compromised by the Data Breach.[12]

29. LabCorp provided AMCA with Sensitive Information about LabCorp's patients in order to facilitate the bill collection process.

30. The patient information LabCorp provided to AMCA, including that of Plaintiff Shulman and the putative Class, included personal and medical information, such as the first and last name, date of birth, address, phone, date of service, service provider, and account balance information.[13]

---

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

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

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

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

31. Upon information and belief, AMCA stored the information LabCorp provided to AMCA in its own computer systems. These same AMCA systems were compromised in the Data Breach.

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

B. Defendant Had a Duty and Obligation to Protect Plaintiff's and Class Members' Sensitive Information from Unauthorized Disclosure.

33. Defendant agreed, and had a duty and obligation, to keep confidential the Sensitive Information their patients disclosed to it and to protect this information from unauthorized disclosure. Defendant's agreement, duties, and obligations are based on: (1) HIPAA; (2) industry standards; and (3) the agreements and promises made to Plaintiff and the putative Class. Class members provided their Sensitive Information to Defendant with the reasonable belief that Defendant and its business affiliates would comply with its agreements and any legal requirements to keep that Sensitive Information confidential and secure from unauthorized disclosure.

34. HIPAA requires that LabCorp provide every patient it treats, including Plaintiff and the putative Class members with a privacy notice.

35. In this HIPAA-mandated privacy notice, LabCorp agrees that it will keep PHI of its patients, including Plaintiff Shulman and the putative Class, confidential and protected from

unauthorized disclosure. In its Notice of Privacy Practices effective May 9, 2016, LabCorp promises and agrees in relevant part[14]:

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

36. LabCorp posts this Notice of Privacy Practices on its website, acknowledging its agreement, duty and promise to protect all PHI in its possession.

37. LabCorp's data security agreement, obligations, and commitments are particularly important given the substantial increase in data breaches (particularly in the healthcare industry) during the period preceding the Data Breach. LabCorp's failure to provide the data-security protections it committed to provide to Plaintiff and members of the putative Class was particularly egregious in light of specific government warnings regarding the possibility of

[14] *HIPAA Information*, LabCorp, https://www.labcorp.com/hipaa-privacy/hipaa-information (last visited June 10, 2019).

attempts to hack companies like LabCorp. Such warnings alerted LabCorp of the risk of a data breach and further emphasized LabCorp's duty to keep patients' Sensitive Information secure.

38. For example, on April 8, 2014, the Federal Bureau of Investigation's Cyber Division issued a Private Industry Notification to companies within the healthcare sector, stating that "the health care industry is not technically prepared to combat against cyber criminals' basic cyber intrusion tactics, techniques and procedures (TTPs), much less against more advanced persistent threats (APTs)" and pointed out that "[t]he biggest vulnerability was the perception of IT healthcare professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise." The same warning specifically noted that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or PII."[15]

39. AMCA was a "business associate" of LabCorp with whom LabCorp shared Sensitive Information. As LabCorp's business associate, AMCA was required to maintain the privacy and security of Plaintiff's and Class members' Sensitive Information. HIPAA mandates that a covered entity may only disclose PHI to a "business associate" if the entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[16]

---

[15] *(U) Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (Apr. 8, 2014), FBI Cyber Division Private Industry Notification, *available at* https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf. .

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

C. Defendant Failed to Properly Protect Plaintiff's and the Putative Class' Sensitive Information.

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

41. The length of time between the breach and AMCA's discovery indicates that AMCA's systems to detect intrusion, detect unusual activity, and log and report such events was inadequate. For example, according to technology-security company FireEye, the median amount of time between when a data breach occurs and when it is detected was 78 days in 2018. This number has consistently been on a downward trend in recent years.[17] The fact that it took AMCA 242 days to detect the Data Breach is evidence of its failure to employ reasonable, industry-standard data-security practices to safeguard Plaintiff's and Class members' Sensitive Information.

42. AMCA's apparent inability to detect the Data Breach on its own, when a third-party security firm (Gemini Advisory—which was *not* working for AMCA) was apparently able to do so with ease, is further evidence of the fact that AMCA employed inadequate data-security practices.

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

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

portal of AMCA, one of the largest recovery agencies for patient collections. Several financial institutions also collaboratively confirmed the connection between the compromised payment card data and the breach at AMCA.[18]

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

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

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

> [LabCorp] has been notified by Retrieval-Masters Creditors Bureau, Inc. d/b/a American Medical Collection Agency (AMCA) about unauthorized activity on AMCA's web payment page (the AMCA Incident). According to AMCA, this activity occurred between August 1, 2018, and March 30, 2019. AMCA is an external collection agency used by LabCorp and other healthcare companies. LabCorp has referred approximately 7.7 million consumers to AMCA whose data was stored in the affected AMCA system. AMCA's affected system included information provided by LabCorp. That information could include first and last name, date of birth, address, phone, date of service, provider, and balance information. AMCA's affected system also included credit card or bank account information that was provided by the consumer to AMCA (for those who sought to pay their balance).[21]

---

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

[19] *Id.*

[20] *Id.*

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

47. LabCorp further disclosed in its SEC filing that "AMCA has informed LabCorp that it is in the process of sending notices to approximately 200,000 LabCorp consumers whose credit card or bank account information may have been accessed. AMCA has not yet provided LabCorp a list of the affected LabCorp consumers or more specific information about them."[22]

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

> We are investigating a data incident involving an unauthorized user accessing the American Medical Collection Agency system," reads a written statement attributed to the AMCA. "Upon receiving information from a security compliance firm that works with credit card companies of a possible security compromise, we conducted an internal review, and then took down our web payments page.
>
> . . . .
>
> We hired a third-party external forensics firm to investigate any potential security breach in our systems, migrated our web payments portal services to a third-party vendor, and retained additional experts to advise on, and implement, steps to increase our systems' security. We have also advised law enforcement of this incident. We remain committed to our system's security, data privacy, and the protection of personal information.[23]

49. In response to AMCA's initial notification of the Data Breach, LabCorp ceased sending new collection requests to AMCA and instructed AMCA to stop working on any pending collection requests involving LabCorp consumers.[24]

---

[22] *Id.*

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

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

50. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). PCI DSS is the industry standard governing the security of payment card data, although it sets the minimum level of what must be done, not the maximum.

51. The payment card industry has published a guide on point-to-point encryption and its benefits in securing payment card data: "point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[25] Had AMCA implemented a P2PE solution prior to the data breach and an attacker were to steal encrypted payment card data, that data would have been commercially worthless to the attacker as the attacker would not be able to decrypt the data to obtain the information necessary to make fraudulent purchases.

52. Gemini found credit card numbers from the breach for sale on the dark web, which means that AMCA did not encrypt those numbers in accordance with PCI DSS.

53. Access to the 11.9 million Quest patient records and 7.7 million LabCorp patient records through AMCA's online portal should not have been possible, had AMCA maintained appropriate protections. The sheer number of records suggests that AMCA was not destroying or archiving inactive records such as Plaintiff's so that they could not be accessed through the

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

internet, a standard practice that likely would have greatly reduced the number of people impacted by this breach.

D. Data Security Breaches Lead to Increased Actual and Potential Identity Theft.

54. Defendant knew or should have known that the Sensitive Information that they were collecting from Plaintiff and members of the putative Class, which was stolen during the Data Breach, was highly valuable and highly sought-after by criminals.

55. There has been an "upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published."[26]

56. The United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report") that identity thieves use personally identifying data to open financial accounts, receive government benefits and incur charges and credit in a person's name.[27] As the GAO Report notes, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

57. In addition, the GAO Report makes clear that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[28]

---

[26] *Healthcare Data Breach Statistics*., HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited June 10, 2019).

[27] *See Personal Information: Data Breaches Are Frequent, But Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* http://www.gao.gov/new.items/d07737.pdf.

[28] *Id*.

58. Identity theft victims must often spend countless hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information such as social security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[29]

59. With access to an individual's Sensitive Information, criminals can do more than just empty a victim's bank account; they can also commit many types of fraud, including: obtaining a driver's license or other official identification card in the victim's name but with the thief's picture on it; using the victim's name and social security number to obtain government benefits; and filing a fraudulent tax return using the victim's PII. In addition, identity thieves may obtain a job using the victim's PII, rent a house or receive medical services, prescription drugs and goods, and cause fraudulent medical bills to be issued in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued against the identity theft victim.[30] Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail and other negative effects.

60. In a data breach implicating a medical provider or medical information, consumers face the additional risk of their Health Savings Accounts ("HSAs") being

[29] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201. 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," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[30] *See Warning Signs of Identity Theft*, Federal Trade Commission, *available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft#What (last visited June 13, 2019).

compromised. HSAs are often tied to specialized debit cards used to make medical-based payments. However, they can also be used for regular purchases (albeit incurring a severe tax penalty).[31] Such information is an "easy target" for criminal actors.[32]

61. Sensitive Information is a valuable commodity to identity thieves. Compromised Sensitive Information is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, social security numbers and other Sensitive Information directly on various dark web[33] sites making the information publicly available.[34]

62. Further, medical databases are particularly high value targets for identity thieves. According to one report, a stolen medical identity has a $50 street value on the black market, whereas a Social Security number sells for only $1.[35]

63. The medical industry has experienced disproportionally higher instances of data breaches than any other industry.[36]

---

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

[32] *Id.*

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

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

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

[36] Bob Kehoe, *Hospitals boost efforts to improve cybersecurity*, Health Facilities Management,

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

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

E. Plaintiff and Putative Class Members Are in Imminent Danger of Identity Theft.

66. Defendant caused harm to Plaintiff and putative Class members by sharing its patients' Sensitive Information with AMCA. LabCorp failed to properly monitor its vendor, and AMCA failed to prevent attackers from accessing and stealing this information in the Data Breach.

67. Criminals steal—and sell—Sensitive Information in order to use it for illicit means. The question is when, not whether, it will be misused. But whether or not the Sensitive Information stolen in the Data Breach is later used in a criminal enterprise, Plaintiff and putative

---

(April 26, 2016), https://www.hfmmagazine.com/articles/2162-hospitals-boost-efforts-to-improve-cybersecurity?dcrPath=%2Ftemplatedata%2FHF_Common%2FNewsArticle%2Fdata%2FHFM%2FHFM-Daily%2F2016%2Fibm-cybersecurity-intelligence-index-health-care (noting that a report from IBM Security "noted that in 2015, health care became the most frequently attacked field, moving ahead of manufacturing and financial services"); *The Healthcare Industry – A Prime Target for Hackers and Data Breaches*, Bluefin, https://www.bluefin.com/bluefin-news/the-healthcare-industry-a-prime-target-for-hackers-and-data-breaches/ (last visited June 12, 2019) ("healthcare is now the most heavily attacked industry").

Class members suffered economic harm as even the mere theft of their Sensitive Information significantly increases the risk of their identity being exploited in ways that can cause economic harm to them. This increased risk decreases the value of their Sensitive Information.

68. Plaintiff and members of the putative Class have experienced fraud at or near the time of the announced Data Breach, including Plaintiff Shulman.

69. Two of Plaintiff Shulman's credit cards have recently shown fraudulent charges. One of Plaintiff Shulman's credit cards showed fraudulent charges approximately in late May 2019, and another card showed fraudulent charges in June 2019. Plaintiff Shulman gave Defendant her credit card information in connection with payment for laboratory testing services.

CLASS ALLEGATIONS

70. Plaintiff Shulman brings this action on behalf of a Nationwide Class, defined respectively as follows:

> LabCorp Nationwide Class: All persons in the United States who utilized services of LabCorp and whose Sensitive Information was maintained on the AMCA systems that were compromised as a result of the Data Breach announced by LabCorp on or around June 4, 2019.

71. To the extent necessary for manageability, Plaintiff proposes, in the alternative to the Nationwide Class, that the Court certify state subclasses that would group together similar causes of action for states requiring similar evidentiary proof. Plaintiff reserves the right to amend the Class definitions if discovery and further investigation reveal that the Class should be expanded, divided into further classes, or modified in any other way. Plaintiff reserves the right to propose other subclasses prior to trial.

72. Excluded from the Class are Defendant, its parents, subsidiaries, agents, officers and directors. Also excluded from the Class is any judicial officer assigned to this case and members of his or her staff.

73. Plaintiff seeks class certification pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3). In the alternative, Plaintiff seeks class certification under Fed. R. Civ. P. 23(c)(4) because the common questions listed herein predominate as to particular issues that could substantially advance the litigation. The proposed Class meets the applicable requirements for certification under Fed. R. Civ. P. 23.

74. **Numerosity**: According to Defendant's public statements, there are approximately 7.7 million individuals in the LabCorp Nationwide Class, making joinder of each individual member impracticable. Ultimately, members of the Class will be easily identified through Defendant's records.

75. **Commonality and Predominance**: Questions of law and fact common to the claims of Plaintiff and the other members of the Class predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant failed to adequately safeguard Plaintiff's and the Class' Sensitive Information;

b. Whether Defendant failed to protect or otherwise keep Plaintiff's and the Class' Sensitive Information secure, as promised;

c. Whether Defendant's storage of Plaintiff's and the Class' Sensitive Information violated HIPAA, federal, state, local laws, or industry standards;

d. Whether Defendant engaged in unfair or deceptive practices by failing to properly safeguard Plaintiff's and the Class' Sensitive Information, as promised;

e. Whether Defendant violated the consumer protection statutes applicable to Plaintiff and the Class;

f. Whether Defendant failed to notify Plaintiff and members of the Class about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

g. Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class' Sensitive Information;

h. Whether Plaintiff and the members of the Class are entitled to damages as a result of Defendant's conduct.

76. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and the members of the Class sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them, including their storage and transmission of the Sensitive Information and failure to adequately safeguard it.

77. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class and have the financial resources to do so. Neither Plaintiff nor her counsel has any interest adverse to those of the other members of the Class.

78. **Risks of Prosecuting Separate Actions**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class.

79. **Policies Generally Applicable to the Class**: This class action is appropriate for certification because Defendant have acted or refused to act on grounds generally applicable to the Plaintiff and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's lax data security protocols and practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenges to those practices hinge on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

80. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if members of the Class could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

II. CAUSES OF ACTION

FIRST CLAIM FOR RELIEF

Negligence
(Against Defendant on Behalf of Plaintiff and the Nationwide Class)

81. Plaintiff incorporates paragraphs 1 – 69 as if fully set forth herein.

82. Defendant required Plaintiff and the Class members to submit Sensitive Information in order to obtain services and in consideration for Plaintiff and class members paying for or using those services.

83. By collecting and storing this data, and by sharing this data with its business associates, LabCorp had a duty of care to use reasonable means to secure and safeguard this Sensitive Information, to prevent disclosure of the information form itself and its vendors, and to guard the information from theft.

84. Defendant LabCorp assumed a duty of care to use reasonable means and implement policies and procedures to prevent unauthorized access to this Sensitive Information.

85. Defendant LabCorp had a duty to monitor, supervise, or otherwise provide oversight to safeguard the Sensitive Information it stored and shared with its business associates and vendors.

86. Furthermore, given the other major data breaches affecting the healthcare and financial industries, Plaintiff and the Class members are part of a well-defined, foreseeable, finite, and discernible group that was at high risk of having their Sensitive Information stolen.

87. Defendant owed a duty to Plaintiff and members of the Class to provide security consistent with industry standards, statutory requirements, and the other requirements discussed herein, and to ensure that their systems and networks—and the personnel responsible for them—adequately protected their patients' or customers' Sensitive Information.

88. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff or the other Class members, on the other hand. The special relationship arose because Plaintiff and the members of the Class entrusted Defendant with their Sensitive Information as part of receiving or paying for laboratory services. Defendant alone was in a position to ensure that its systems, as well as those of its vendors and business associates, were sufficient to prevent or minimize a Data Breach.

89. Defendant's duty to use reasonable security measures also arose under HIPAA, pursuant to which Defendant was required to "reasonably protect" PHI from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Plaintiff's and Class members' Sensitive Information that was compromised in the Data Breach includes PHI, such as provider names, dates of service, medical billing information and potentially other "protected health information" within the meaning of HIPAA.

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

91. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the common law and the statutes and regulations described above, but also because it was bound by, and had committed to comply with, industry standards for the protection of confidential Sensitive Information.

92. Defendant knew or should have known that AMCA's web payments page was vulnerable to unauthorized access.

93. Defendant breached its common law, statutory and other duties—and thus, was negligent—by failing to use reasonable measures to protect consumers' Sensitive Information from hackers, failing to limit the severity of the Data Breach, and failing to detect the Data Breach in a timely fashion.

94. It was foreseeable that Defendant's failure to use reasonable measures to protect consumers' Sensitive Information, including PII, from attackers, failure to limit the severity of the Data Breach, and failure to detect the Data Breach in a timely fashion, would result in injury to Plaintiff and the members of the Class. Further, the breach of security, unauthorized access, and resulting injuries to Plaintiff and the Class were reasonably foreseeable, particularly in light of the other major data breaches affecting the healthcare and financial industries, including previous attacks at LabCorp.

95. It was therefore reasonably foreseeable that Defendant's breaches of duties and failure to adequately safeguard Sensitive Information would, and in fact did, result in one or more of the following injuries to Plaintiff and the Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit

scores and ratings; lost work time; lost value of the Sensitive Information; and other economic and non-economic harm.

96. Accordingly, Plaintiff, on behalf of herself and members of the Class, seeks an order declaring that Defendant's conduct constitutes negligence, and awarding damages in an amount to be determined at trial.

SECOND CLAIM FOR RELIEF

Violation of North Carolina Unfair and Deceptive Trade Practices Act N.C. Gen. Stat. § 75-1.1, *et seq.* (Against Defendant on Behalf of Plaintiff and the Nationwide Class)

97. Plaintiff incorporates paragraphs 1–69 as if fully set forth herein.

98. Under the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. § 75-1.1, "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful."

99. At all relevant times material hereto, Defendant conducted trade or commerce, or furnished services in the State of North Carolina.

100. Defendant, while operating in North Carolina, engaged in deceptive acts and practices in the conduct of business activities, trade and commerce, in violation of N.C. Gen. Stat. § 75-1.1, because:

a. Defendant failed to enact adequate privacy and security measures to protect the Class Members' Sensitive Information from unauthorized disclosure, release, data breach or theft;

b. Defendant failed to take proper action to address known security risks;

c. Defendant made false or misleading misrepresentations that they would maintain adequate data privacy and security practices and procedures to

safeguard the Sensitive Information from unauthorized disclosure, release, data breach or theft;

d. Defendant failed to disclose, omitted, actively concealed the material fact of the inadequacy of their data security or the true characteristics and quality of their data security;

e. Defendant failed to disclose, omitted, actively concealed the material fact of their reliance on AMCA's inadequate data security; and

f. Defendant made false or misleading misrepresentations that that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Sensitive Information including but not limited to duties imposed by HIPAA.

101. The above listed acts were deceptive because they were likely to mislead a reasonable consumer acting reasonably under the circumstances, and such acts were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the proposed Class members.

102. As set out above, because only Defendant knew (or should have known) that they were not complying with their own data security representations and obligations, there was no way for members of the public, including Plaintiff and members of the proposed Class, to avoid the injury caused by Defendant's conduct. Defendant's failure to use adequate data security practice and failure live up to its data security representations and obligations did not create any countervailing benefits.

103. Plaintiff and the proposed Class members reasonably expected that Defendant would protect their Sensitive Information and provide truthful statements regarding their privacy policies.

104. Defendant engaged in omission of material facts, deception, active concealment, and misrepresentation with the intent that Plaintiff and the putative Class would rely on the same when providing Sensitive Information to Defendant.

105. Defendant's failure to disclose its actual (and substandard) security practices substantially injured the public because it caused millions of consumers to enter into transactions they otherwise would not have, and because it compromised the integrity of Plaintiff's and the Class's Sensitive Information. Further, Defendant's use of substandard security did not create any benefits sufficient to outweigh the harm it caused.

119. Defendant's deceptive acts or practices and general course of conduct is injurious to the public interest, and such acts are ongoing and/or have a substantial likelihood of being repeated inasmuch as the long-lasting harmful effects of their misconduct may last for years (e.g., affected individuals could experience identity theft for years). As such, Defendant's violations present a continuing risk to Plaintiff and the proposed Class members, as well as to the general public.

106. As a result of Defendant's conduct, Plaintiff and members of the Class have suffered actual damages, including the lost value of their Sensitive Information; the lost value of their personal data and lost property in the form of their breached and compromised Sensitive Information (which is of great value to third parties); ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss

of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

107. Plaintiff seeks relief under N.C. Gen. Stat. § 75-16, including but not limited to actual damages in an amount to be proven at trial, treble damages, and reasonable attorney's fees and costs. The amount of such damages is to be determined at trial.

108. Plaintiff also seeks to enjoin Defendant from its deceptive acts and practices described above. Each Class Member will be irreparably harmed unless the Court enjoins Defendant's unlawful, deceptive actions in that Defendant will continue to fail to protect Sensitive Information, including PII, entrusted to them, as detailed herein.

109. In the event that North Carolina law is not applied, Defendant's actions, as complained of herein, constitute unfair, unconscionable, deceptive or fraudulent acts or practices in violation of the consumer protection statues of each of the fifty states.

III. REQUEST FOR RELIEF

Plaintiff, on behalf of herself and the Class, respectfully requests that this Court enter an Order:

1. Certifying this case as a class action on behalf of Plaintiff and the Class defined above, appointing Plaintiff as Class Representatives of the Class, and appointing Plaintiff's counsel to represent the Class;

2. Awarding Plaintiff and Class Members appropriate relief, including actual, punitive and statutory damages;

3. Awarding equitable, injunctive, and declaratory relief as may be appropriate, including without limitation an injunction and declaring Defendant's conduct to be unlawful;

4. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

5. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable by law;

6. Permitting Plaintiff and the Class to amend their pleadings to conform to the evidence produced at trial; and

7. For trial by jury;

8. Awarding such other and further relief as equity and justice may require.

Dated: June 19, 2019

Respectfully submitted,

By: /S/ *David M. Wilkerson*

David M. Wilkerson
NC State Bar No. 35742
Larry McDevitt
NC State Bar No. 5032
THE VAN WINKLE LAW FIRM
11 North Market Street
Asheville, NC 28801
Tel: (828) 258-2991
Email: dwilkerson@vwlawfirm.com
lmcdevitt@vwlawfirm.com

James Pizzirusso*
HAUSFELD LLP
1700 K. Street NW, Suite 650
Washington, DC 20006
Tel: (202) 540-7200
Fax: (202) 540-7201
Email: jpizzirusso@hausfeld.com

Kim D. Stephens*
Jason T. Dennett*
Cecily C. Shiel*
TOUSLEY BRAIN STEPHENS, PLLC
1700 Seventh Avenue, Suite 2200
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992
Email: kstephens@tousley.com
jdennett@tousley.com
cshiel@tousley.com

Daniel L. Warshaw*
PEARSON, SIMON & WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, California 91403
Tel: (818) 788 8300
Fax: (818) 788 8104
Email: dwarshaw@pswlaw.com

Melissa S. Weiner*
Joseph C. Bourne *
PEARSON, SIMON & WARSHAW, LLP
800 LaSalle Avenue, Suite 2150
Minneapolis, Minnesota 55402
Tel: (612) 389-0600
Fax: (612) 389-0610
Email: mweiner@pswlaw.com
jbourne@pswlaw.com

Attorneys for Plaintiff and the Proposed Class

**Pro hac vice* applications forthcoming