EFiled: Apr 28 2020 03:30PM EDT
Transaction ID 65604938
Case No. 2020-0305-PAF

IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

RAYMOND EUGENIO, Derivatively on Behalf of Nominal Defendant, LABORATORY CORPORATION OF AMERICA HOLDINGS, Plaintiff, vs. LANCE V. BERBERIAN, GLENN A. EISENBERG, ADAM H. SCHECHTER, KERRII B. ANDERSON, JEAN-LUC BÉLINGARD, JEFFREY DAVIS, D. GARY GILLILAND, M.D., PH.D., DAVID P. KING, GARHENG KONG, M.D., PH.D., PETER M. NEUPERT, RICHELLE P. PARHAM, and R. SANDERS WILLIAMS, M.D., Defendants, and LABORATORY CORPORATION OF AMERICA HOLDINGS, Nominal Defendant.	C.A. No. 2020-0305-PAF

VERIFIED SHAREHOLDER DERIVATIVE COMPLAINT

Plaintiff Raymond Eugenio ("Plaintiff"), by and through his undersigned attorneys, submits this Verified Shareholder Derivative Complaint (the "Complaint") against defendants named herein. Plaintiff alleges the following based upon information and belief, except as to those allegations concerning Plaintiff, which are alleged upon personal knowledge. Plaintiff's information and belief is based upon, among other things, the investigation conducted by and under the supervision of his counsel which included, among other things: (a) a review and analysis of regulatory filings filed by Laboratory Corporation of America Holdings ("LabCorp" or the "Company") with the United States Securities and Exchange Commission ("SEC"); (b) documents produced by LabCorp pursuant to 8 Del. C. § 220; (c) a review and analysis of press releases and media reports issued and disseminated by LabCorp; (d) a review of other publicly available information concerning LabCorp, including articles in the news media and analyst reports; (e) complaints and related materials in litigation commenced against some or all of the Individual Defendants (defined below) and/or the Company; and (f) applicable rules and regulations.

SUMMARY OF THE ACTION

1. This is a shareholder's derivative action brought for the benefit of Nominal Defendant LabCorp, a publicly traded company, against current members of the Company's Board of Directors (the "Board" or "Director Defendants") and

certain of its current executive officers (the "Officer Defendants") (collectively, the "Individual Defendants") seeking to remedy the Individual Defendants' violations of federal and state law and breaches fiduciary duty.

2. On February 28, 2019, analysts from cybersecurity firm Gemini Advisory ("Gemini") identified a large number of compromised payment cards located on the "dark web," which contained personally identifiable information ("PII") and potentially personal health information ("PHI"). Based on the analysis performed by Gemini, the information found on the dark web was likely stolen from American Medical Collection Agency ("AMCA"), a debt collector that engaged in collecting patient receivables for medical labs. Additionally, several financial institutions confirmed the connection between the compromised payment card data and AMCA.

3. Gemini unsuccessfully attempted to inform AMCA of the compromised payment information located on the dark web. After failing to obtain a satisfactory response from AMCA, Gemini contacted federal authorities to ensure that AMCA was made aware of the connection between the compromised payment information and AMCA.

4. Upon further analysis and investigation, AMCA determined that there was a breach of AMCA's payment portal which occurred from August 1, 2018 through March 30, 2019 (the "AMCA Incident"). In response to the AMCA

Incident, AMCA rendered its payment portal inoperable until May 2019.

5. On May 14, 2019, AMCA informed LabCorp that there was a breach of AMCA's web payment page. The data breach, which lasted nearly eight (8) months, directly impacted and affected millions of LabCorp patients (the "First Breach"). LabCorp failed to immediately make a public disclosure after learning of the First Breach. Instead, the Company waited until June 4, 2019 to inform LabCorp investors of the First Breach through an SEC filing.

6. After publicly disclosing the First Breach, LabCorp immediately began receiving inquiries from United States Senators, state attorneys general, and federal and state agencies regarding the First Breach. Some of these inquiries referenced the Company's historically deficient data and cybersecurity controls. LabCorp received a letter from United States Senator Robert Menendez and United States Senator Cory A. Booker requesting information regarding the First Breach and raising concerns over LabCorp's previous issues with cybersecurity. Specifically, the United States Senators stated, in part:

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

processes to better protect the patients it serves.

(Emphasis added).

7. Even in the face of multiple inquiries regarding the First Breach, LabCorp and the Individual Defendants knowingly and intentionally refrained from providing notice to affected LabCorp patients in relation to the First Breach. [redacted]

8. As of today, estimates suggest that more than 10.2 million LabCorp patients have had their personal information compromised as a result of the First Breach.

9. Once again, in early 2020, LabCorp's historically and persistently deficient cybersecurity measures were on display. On January 28, 2020, LabCorp

[1] References to "LCA____" refers to bates stamped documents produced by Defendants pursuant to 8 Del. C. § 220.

was informed of a second data breach in which an unprotected web address granted access to LabCorp documentation containing PHI (the "Second Breach" and, collectively with the First Breach, the "Data Breaches"). The same day, *TechCrunch* published an article (the "*TechCrunch* Article") describing the Second Breach and indicating that "at least 10,000 documents were exposed." LabCorp has not publicly responded to or acknowledged the media reports of the Second Breach. *TechCrunch*, however, indicates that the vulnerability on LabCorp's website has been corrected.

10. Subsequent to the publication of the *TechCrunch* Article, the Company indicated that it would provide notice to affected LabCorp patients "as may be appropriate," but would not disclose whether the Company would inform state and local authorities.

11. The Second Breach was never disclosed by the Company or the Individual Defendants in any SEC filing or other widely disseminated public disclosure. Moreover, beyond the post-publication statement provided to *TechCrunch*, neither LabCorp nor the Individual Defendants have publicly acknowledged that the Second Breach even occurred.

12. LabCorp's insufficient cybersecurity procedures and oversight of AMCA, a business associate (as defined below), permitted unauthorized access to LabCorp patients' confidential, personal information. Amongst the stolen

information in the Data Breaches was the person's name, addresses, dates of birth, Social Security numbers, medical information, payment information, credit card numbers, account information, and other highly sensitive information.

13. As a result of the First Breach, the Company is now subject to a Consolidated Class Action Complaint ("Consumer Class Action") currently pending in the United States District Court for the District of New Jersey, *American Medical Collection Agency, Inc., Customer Data Security Breach Litigation*, Docket No. 19-md-2904 (MCA)(MAH) (D.N.J. filed July 31, 2019), brought on behalf of LabCorp patients who had personal information compromised in the First Breach.

14. The Consumer Class Action consolidates claims made by numerous plaintiffs throughout the United States and raises, *inter alia*, claims for negligence, negligence per se, unjust enrichment, breach of contract, and multiple violations of state health care information acts, privacy acts, and identity theft protection acts.

15. Prior to and subsequent to the First Breach, LabCorp continued to have insufficient cybersecurity procedures and oversight that permitted a malware attack in July 2018 (the "2018 Malware Attack") and the Second Breach, which occurred approximately nine (9) months after the First Breach.

16. As a consequence of the First Breach, LabCorp disclosed that the Company spent $11,500,000 during 2019 for response and remediation costs. The amount disclosed by LabCorp does not include or contemplate the extensive

litigation costs resulting from the First Breach. Additionally, the Company has not disclosed how much it anticipates the First Breach to cost in subsequent years. LabCorp has also not disclosed any costs associated with the Second Breach or any anticipated costs.

17. Demand is futile in this case as there does not exist a majority of Board members capable of disinterestedly and independently considering a demand. Amongst other reasons, demand is futile because the Board consciously disregarded its duties to provide timely notice of the Data Breaches to affected individuals, knowingly failed to make adequate public disclosures of the Data Breaches, willfully and intentionally disregarded the Company's obligations to increase and/or establish more effective cybersecurity policies and procedures, and sought to disclaim all liability and responsibility for LabCorp patient data by, in effect, levying all accountability and remedial actions upon AMCA for the First Breach and then outright ignoring the ramifications of the Second Breach.

18. The Individual Defendants breached their duties of loyalty, care, and good faith by: (i) failing to implement and enforce a system of effective internal controls and procedures to protect patients' PII and PHI; (ii) failing to exercise their oversight duties by not monitoring the Company's compliance with its own procedures and federal and state regulations; (iii) providing PII and PHI of patients to a business associate with deficient cybersecurity and breach detection; (iv) failing

to ensure that the Company, as well as its business associates, utilized proper cybersecurity safeguards to adequately secure the PII and PHI; (v) failing to have a sufficient incident response plan to immediately respond to the Data Breaches; (vi) consciously disregarding, delaying, and failing to ensure that the Company notified all potentially affected individuals and entities in a timely manner upon discovering the Data Breaches; (vii) failing to make adequate public disclosure of the Data Breaches; and (viii) allowing the Company to violate state and federal laws and regulations.

JURISDICTION AND VENUE

19. This Court has jurisdiction over this action pursuant to 10 Del. C. § 341.

20. As officers and directors of a Delaware corporation, the Individual Defendants have consented to jurisdiction of this Court pursuant to 10 Del. C. § 3114.

21. This Court has jurisdiction over LabCorp pursuant to 10 Del. C. § 3111.

PARTIES

22. Plaintiff Raymond Eugenio is currently and has continuously been a stockholder of LabCorp since June 28, 2013. Plaintiff is a citizen of the State of New Jersey.

23. Nominal Defendant LabCorp is incorporated under the laws of Delaware and maintains its headquarters in Burlington, North Carolina. According

to the Company's website, LabCorp was established in 1995 through the merger of Roche Biomedical Laboratories ("Roche") and National Health Laboratories ("National Health"). National Health was a publicly traded company, listed on NASDAQ since 1988. Roche was one of the largest clinical laboratory networks in the United States, with 20 major laboratories and $600 million in sales during the early 1990s. According to the Company's Form 10-Q for the period ended March 31, 1995, filed with the SEC on May 15, 1995, on April 28, 1995 National Health changed the name of the Company to LabCorp and completed the merger with Roche. LabCorp continues to trade under the ticker symbol LH. LabCorp together with its subsidiaries operates one of the largest clinical laboratory networks in the world.

Lance V. Berberian

24. Defendant Lance V. Berberian ("Berberian") is the Company's Chief Information and Technology Officer ("CITO"). According to LabCorp's DEF 14A Proxy Statement filed with the SEC on April 1, 2020 (the "2020 Proxy Statement"), Berberian has served as the CITO of the Company since February 2014.

25. According to the 2020 Proxy Statement, as of July 1, 2019, Berberian receives a base salary of $515,000. According to the 2020 Proxy Statement, in 2019 Berberian received total compensation of $2,703,124. This included $507,500 in salary, $151,375 in stock options, $1,675,133 in stock awards, $359,311 in non-

equity incentive plan compensation, and $9,805 of other compensation.

26. According to the 2020 Proxy Statement, Berberian beneficially owns 18,904 shares of the Company's common stock.

27. The Company's 2020 Proxy Statement stated the following about Defendant Berberian:

> Lance V. Berberian (57) has served as Executive Vice President and Chief Information and Technology Officer since February 15, 2020. Prior to that he served as Senior Vice President and Chief Information Officer from February 2014. Mr. Berberian served as Chief Information Officer at IDEXX Laboratories, a global leader in diagnostics and information technology solutions for animal health and food and water quality, from May 2007 to January 2014. Mr. Berberian served as Chief Information Officer and President of Kellstrom Aerospace Defense, a fully integrated supply chain firm, from January 2000 to April 2007. He also served as Chief Information Officer of Interim Healthcare from September 1997 to January 2000.

Glenn A. Eisenberg

28. Defendant Glenn A. Eisenberg ("Eisenberg") is the Company's Chief Financial Officer ("CFO"). According to the 2020 Proxy Statement, Eisenberg has served as the CFO of the Company since June 2014.

29. According to the 2020 Proxy Statement, in 2019 Eisenberg received total compensation of $8,822,761. This included $705,500 in salary, $399,081 of options, $6,966,915 of stock awards, $715,540 of non-equity incentive plan compensation, and $35,725 in other compensation. According to the 2020 Proxy Statement, in 2018 Eisenberg received total compensation of $3,430,739. This

included $686,662 in salary, $403,747 of options, $1,666,134 of stock awards, $621,241 of non-equity incentive plan compensation, and $52,955 in other compensation. According to the 2020 Proxy Statement, in 2017 Eisenberg received total compensation of $3,407,745. This included $666,474 in salary, $373,349 of options, $1,588,668 of stock awards, $746,219 of non-equity compensation, and $33,035 in other compensation.

30. According to the 2020 Proxy Statement, Eisenberg beneficially owns 53,243 shares of the Company's common stock.

31. According to the 2020 Proxy Statement, in 2019, the Compensation Committee determined that Eisenberg should receive a special restricted stock award valued at approximately $5,000,000.

32. The Company's 2020 Proxy Statement stated the following about Defendant Eisenberg:

> Glenn A. Eisenberg (58) has served as Executive Vice President and Chief Financial Officer since June 2014. Mr. Eisenberg received his Bachelor of Arts degree from Tulane University in 1982 and his Master of Business Administration from Georgia State University in 1988. From 2002 until joining the Company, he served as the Executive Vice President of Finance and Administration and Chief Financial Officer at The Timken Company, a $4.3 billion leading global manufacturer of highly engineered bearings and alloy steels and related products and services. Previously, he served as President and Chief Operating Officer of United Dominion Industries, now a subsidiary of SPX Corporation, after working in several roles in finance, including Executive Vice President and Chief Financial Officer. Mr. Eisenberg serves on the Board of Directors of US Ecology, Inc. (NASDAQ: ECOL) since December 2018, and as a director of Perspecta Inc.

> (NYSE: PRSP) since May 2019. Mr. Eisenberg served on the Boards of Directors of Family Dollar Stores Inc. until July 2015, where he chaired the Audit Committee; and Alpha Natural Resources Inc. until May 2015, where he was the lead independent director and chaired the Nominating and Corporate Governance Committee.

Adam H. Schechter

33. Defendant Adam H. Schechter ("Schechter") has been a director of the Company since April 2013. Schechter began serving as the Company's President and Chief Executive Officer ("CEO") effective November 1, 2019.

34. According to the Company's 2020 Proxy Statement, in 2019 Schechter received total compensation of $4,617,739. This included $208,333 in salary, $2,966,978 in stock options, $1,002,511 in stock awards, $321,691 of non-equity incentive compensation, and $118,226 in other compensation. Additionally, prior to Schechter's appointment as CEO, Schechter received $105,000 in cash and $179,866 in stock awards for services rendered as a director of the company.

35. Schechter beneficially owns 7,689 shares of the Company's common stock.

36. The Company's 2020 Proxy Statement stated the following about Defendant Schechter:

> Adam H. Schechter has served as a director of the Company since April 1, 2013 and as the President and Chief Executive Officer of the Company since November 1, 2019. Prior to that, Mr. Schechter was an Executive Vice President of Merck & Co., Inc. from 2010 to 2018, where he was a member of Merck's executive committee and pharmaceutical and vaccines operating committee. He served as special

> advisor to the CEO of Merck from January 2019 to July 2019. He previously served as President of Merck's Global Human Health Division, which includes the company's worldwide pharmaceutical and vaccine businesses from 2010 to 2018. Prior to becoming President, Global Human Health, Mr. Schechter served as President, Global Pharmaceutical Business from 2007 to 2010. Mr. Schechter's extensive experience at Merck included global and U.S.-focused leadership roles spanning sales, marketing, and managed markets, as well as business and product development. He is a Board Member for Water.org and an executive board member for the National Alliance for Hispanic Health.

Kerrii B. Anderson

37. Defendant Kerrii B. Anderson ("Anderson") has been a director of the Company since May 2016. Anderson serves as LabCorp's Audit Committee chairperson and is a member of the Nominating and Corporate Governance Committee.

38. According to the Company's 2020 Proxy Statement, in 2019 Anderson received total compensation of $314,866. This included $135,000 in cash and $179,866 in stock awards.

39. According to the Company's 2020 Proxy Statement, Anderson beneficially owns 20,360 shares of the Company's common stock.

40. The Company's 2020 Proxy Statement stated the following about Defendant Anderson:

> Kerrii B. Anderson has served as a director of the Company since May 17, 2006. Ms. Anderson was Chief Executive Officer of Wendy's International, Inc., a restaurant operating and franchising company, from April 2006 until September 2008, when the company was merged with Triarc. Ms. Anderson served as Executive Vice President and

> Chief Financial Officer of Wendy's International from 2000 to 2006. Prior to this position, she was Chief Financial Officer, Senior Vice President of M/I Schottenstein Homes, Inc. from 1987 to 2000. Ms. Anderson has served as a director and a member of the Compensation Committee and Audit Committee of Worthington Industries, Inc. (NYSE: WOR) since September 2010, a director and member of the Audit and Finance Committee of Abercrombie & Fitch Co. (NYSE: ANF) since February 2018, and a director and a member of the Compensation and Management Development Committee of The Sherwin-Williams Company (NYSE: SHW) since April 2019. Ms. Anderson serves on the Financial Committee of the Columbus Foundation and on the Board of Trustees, as well as the Chair of the Finance and Audit Committee for Ohio Health. She serves on the Board of Trustees for Elon University and is Chairwoman of the Audit Committee for Elon. Ms. Anderson served as the Chairwoman of the board of Chiquita Brands International Inc. from October 2012 until the Company was sold on January 6, 2015, and was the chair of the Nominating and Corporate Governance Committee and a Member of the Audit Committee. She also was a director of PF Chang's China Bistro, Inc. from 2010 until June 2012 and Wendy's International from 2006 until September 30, 2008.

Jean-Luc Bélingard

41. Defendant Jean-Luc Bélingard ("Bélingard") has served as a director of the Company since April 1995. Bélingard serves as a member of LabCorp's Compensation Committee and Quality and Compliance Committee.

42. According to the Company's 2020 Proxy Statement, in 2019 Bélingard received total compensation of $289,866. This included $110,000 in cash and $179,866 in stock awards. According to LabCorp's DEF 14A Proxy Statement filed with the SEC on March 29, 2019 (the "2019 Proxy Statement"), in 2018 Bélingard received total compensation of $749,975. This included $106,250 in cash and

$643,725 in stock awards. Bélingard's stock award included a "discretionary equity award of 3,271 shares" of the Company's common stock. Specifically, the 2019 Proxy Statement states the following about this "Extraordinary Award":

> This amount includes a one-time discretionary equity award of 3,271 shares granted on December 4, 2018 at a fair value price of $468,832 by the Board to Mr. Bélingard (the "Extraordinary Award"). The Board made the Extraordinary Award after considering special circumstances that resulted in the expiration of an option award held by Mr. Bélingard for 5,300 shares at an exercise price of $75.63 in May of 2018 (the "Prior Option").

43. According to the 2020 Proxy Statement Bélingard beneficially owns 17,282 shares of the Company's common stock.

44. The Company's 2020 Proxy Statement stated the following about Defendant Bélingard:

> Jean-Luc Bélingard has served as a director of the Company since April 28, 1995. Mr. Bélingard currently serves as Operating Advisor to Clayton, Dubilier & Rice, a private equity investment firm, since October 2019. From 2011 to December 2017, Mr. Bélingard served as Chairman and CEO of bioMérieux (Président Directeur Général), the worldwide leader of the IVD microbiology segment and a non-U.S. public company. Mr. Bélingard continues to serve on the board of directors of bioMérieux and as Vice President of Institut Mérieux. Mr. Bélingard retired as Chairman and Chief Executive Officer of Ipsen SA, a diversified French healthcare holding company, on November 22, 2010. He had served in that position since 2002. Prior to this position, Mr. Bélingard was Chief Executive Officer from 1999 to 2001 of bioMérieux-Pierre Fabre, a diversified French healthcare holding company, where his responsibilities included the management of that company's worldwide pharmaceutical and cosmetic business. From 1990 to 1999, Mr. Bélingard was Chief Executive Officer of Roche Diagnostics and a member of the Hoffman La Roche group Executive Committee. Mr. Bélingard is a director of Lupin Limited (India), a non-

> U.S. public company. Mr. Bélingard is also a director at Transgene SA an Institut Mérieux company. Mr. Bélingard serves on the board of Laboratoire Pierre Fabre S.A. (France) since 2013, which is owned by The Pierre Fabre Foundation, a government-recognized public organization. Mr. Bélingard is also a member of the Bill and Melinda Gates Foundation CEO Roundtable and has served on the Novo Advisory Group of Novo Holdings since 1998. Mr. Bélingard was Chairman of "FEFIS," the French Federation of Health Industries (Fédération Française des Industries de Santé) from 2016 to December 2019, and, since January 2017, he has been a member of the Conseil National de l'Industrie (C.N.I.) chaired by the French government. Mr. Bélingard's long tenure at Roche, Ipsen and bioMérieux demonstrates his valuable business, leadership and management experience, including leading a large healthcare organization with global operations. He brings a strong strategic, operational and risk management background to the Company's Board and an important international perspective to the board's deliberations. In addition, Mr. Bélingard has extensive corporate governance experience through his service on other public company boards.

Jeffrey Davis

45. Defendant Jeffrey Davis ("Davis") has served as a director of the Company since December 2019. Davis serves as a member of LabCorp's Audit Committee and Quality and Compliance Committee.

46. According to the Company's 2020 Proxy Statement, in 2019 Davis received total compensation of $39,126. This includes $9,266 in cash and $29,860 in stock awards.

47. The Company's 2020 Proxy Statement stated the following about Defendant Davis:

> Jeffrey A. Davis has served as a director of the Company since December 1, 2019. Mr. Davis currently serves as the Chief Financial

> Officer of Qurate Retail Group, a leading retailer and media conglomerate comprised of eight retail brands including QVC, HSN and Zulily, since October 2018. Prior to Qurate Retail Group, Mr. Davis served as Chief Financial Officer of J. C. Penney Company Inc., from July 2017 until September 2018. Prior to joining J. C. Penney, Mr. Davis served as Chief Financial Officer of Darden Restaurants Inc. from July 2015 until March 2016 and Chief Financial Officer of the Walmart U.S. segment of Walmart Inc. from January 2014 to May 2015, and in various other positions of increasing responsibility at Walmart U.S. from 2006 to 2013. Mr. Davis' experience also includes nine years in senior executive roles at Lakeland Tours LLC and McKesson Corporation. Mr. Davis holds a bachelor's degree in accounting from the Pennsylvania State University and a master's degree in business administration from the Joseph M. Katz Graduate School of Business at the University of Pittsburgh. Mr. Davis' extensive experience in public company leadership and as a CFO across multiple industries brings comprehensive financial management experience to the Board, as well as experience in mergers and acquisitions, capital structure, financial planning and expertise in management.

D. Gary Gilliland, M.D., Ph.D.

48. Defendant D. Gary Gilliland, M.D., Ph.D. ("Gilliland") has served as a director of the Company since April 2014. Gilliland serves as a member of LabCorp's Audit Committee and Quality and Compliance Committee.

49. According to the Company's 2020 Proxy Statement, in 2019 Gilliland received total compensation of $289,866. This included $110,000 in cash and $179,866 in stock awards.

50. According to the Company's 2020 Proxy Statement Gilliland beneficially owns 5,766 shares of the Company's common stock.

51. The Company's 2020 Proxy Statement states the following about

Defendant Gilliland:

> D. Gary Gilliland has served as a director of the Company since April 1, 2014. Dr. Gilliland has served as President and Director Emeritus of the Fred Hutchinson Cancer Research Center in Seattle, WA since January 31, 2020. From January 2, 2015 to January 30, 2020, Dr. Gilliland previously served as President and Director of the Fred Hutchinson Cancer Research Center. Prior to that, he was the inaugural Vice Dean and Vice President for Precision Medicine at the University of Pennsylvania Perelman School of Medicine from October 2013 to January 2015, where he was responsible for synthesizing research and clinical-care initiatives across all medical disciplines including cancer, heart and vascular medicine, neurosciences, genetics, and pathology, to create a national model for the delivery of precise, personalized medicine. From 2009 until he joined Penn Medicine in 2013, Dr. Gilliland was Senior Vice President of Merck Research Laboratories and Oncology Franchise Head. At Merck, Dr. Gilliland oversaw first-in-human studies, proof-of-concept trials, and Phase II/III registration trials that included the development of pembrolizumab (anti-PD1) for treatment of cancer, and managed all preclinical and clinical oncology-licensing activities. Prior to joining Merck, Dr. Gilliland was a member of the faculty at Harvard Medical School for nearly 20 years, where he served as Professor of Medicine and a Professor of Stem Cell and Regenerative Biology. He was also an Investigator of the Howard Hughes Medical Institute from 1996 to 2009, Director of the Leukemia Program at the Dana-Farber/Harvard Cancer Center from 2002 to 2009, and Director of the Cancer Stem Cell Program of the Harvard Stem Cell Institute from 2004 to 2009. Dr. Gilliland has a Ph.D. in Microbiology from UCLA and an M.D. from UCSF. He is board-certified in Internal Medicine and had his Fellowship training in Hematology and Oncology, each at Harvard Medical School. Dr. Gilliland's expertise in cancer genetics and his experience working within medical communities ranging from academia to the pharmaceutical industry position him to provide a practical and balanced perspective to the Board. Dr. Gilliland also brings to the board executive experience in clinical research, as well as in healthcare finance and mergers and acquisitions.

David P. King

52. Defendant David P. King ("King") has served as executive chairman of the Board and director since November 2019. Prior to King's election as a director of the Company, King served as chairman, president, and CEO of LabCorp since May 2009.

53. According to the Company's 2020 Proxy Statement, King beneficially owns 480,995 shares of the Company's common stock.

54. According to the 2020 Proxy Statement, in 2019, King received total compensation of $12,933,590. This included $1,215,000 in salary, $1,799,303 in stock options, $7,676,459 in stock awards, $1,847,880 in non-equity compensation, $224,723 in pension value, and $170,225 in other compensation. According to the 2020 Proxy Statement, in 2018, King received total compensation of $12,264,236. This included $1,175,000 in salary, $1,819,080 in stock options, $7,496,575 in stock awards, $1,584,513 of non-equity compensation, and $189,068 in other compensation. According to the 2020 Proxy Statement, in 2017, King received total compensation of $11,646,254. This included $1,150,000 in salary, $1,581,820 of stock options, $6,749,173 in stock awards, $1,960,367 of nonequity compensation, $128,904 in pension value, and $75,990 in other compensation.

55. According to the Company's 2020 Proxy Statement, King is set to retire on May 13, 2020 at the conclusion of his current term.

56. The Company's 2019 Proxy Statement stated the following about

Defendant King:

> Mr. King has served as Chairman of the Board, President, and Chief Executive Officer of the Company since May 6, 2009; prior to that date he served as a Director, President and Chief Executive Officer of the Company since January 1, 2007. Mr. King served as Executive Vice President and Chief Operating Officer from December 2005 to January 2007, as Executive Vice President of Strategic Planning and Corporate Development from January 2004 to December 2005 and originally joined the Company in September 2001 as Senior Vice President, General Counsel, and Chief Compliance Officer. Prior to joining the Company, he was a partner with Hogan & Hartson LLP (now Hogan Lovells US LLP) in Baltimore, Maryland from 1992 to 2001. He also sits on the Boards of Directors of the Seattle Science Foundation, the American Clinical Laboratory Association, the Emily Krzyzewski Center, and Path, Inc., where he has served as Board Chair since January 2018. Mr. King is also on the Board of Trustees of Elon University. Mr. King also served on the Board of Directors of Cardinal Health Inc., a public company, from 2011 until 2018.

Garheng Kong, M.D., Ph.D.

57. Defendant Garheng Kong, M.D., Ph.D. ("Kong") has served as a director since December 2013. Kong serves as the chairperson of LabCorp's Compensation Committee and is a member of the Nominating and Corporate Governance Committee.

58. According to the Company's 2020 Proxy Statement, in 2019 Kong received total compensation of $309,866. This included $130,000 in cash and $179,866 in stock awards.

59. According to the Company's 2020 Proxy Statement, Kong beneficially owns 8,452 shares of the Company's common stock.

60. The Company's 2020 Proxy Statement stated the following about Defendant Kong:

> Dr. Kong has served as a director of the Company since December 1, 2013. Dr. Kong is the managing partner of HealthQuest Capital, a healthcare-focused investment firm, and was previously a general partner at Sofinnova Capital, a position he held from 2010 to 2013. Before joining Sofinnova, Dr. Kong was a general partner from 2000 to 2010 at Intersouth Partners, a venture capital firm where he was a founding investor or board member for various life science ventures, several of which were acquired by large pharmaceutical companies. Prior to his investing career, Dr. Kong was employed by GlaxoSmithKline, McKinsey & Company, and TherOx. Dr. Kong has served on the board of directors of Venus Concept Inc. (NASDAQ: VERO), a medical technology company, since June 2017, when HealthQuest made an investment in Venus Concept. Dr. Kong has served on the board of directors of Alimera Sciences, Inc. (NASDAQ: ALIM), a pharmaceutical company that specializes in the commercialization and development of ophthalmic pharmaceuticals, since October 2012, when Sofinnova made an investment in Alimera, where he also served as the Chairman of the Compensation Committee. Dr. Kong has served on the board of directors of Strongbridge Biopharma plc (NASDAQ: SBBP) since 2015. Dr. Kong has previously served on the board of directors of Histogenics Corporation (NASDAQ: HSGX) a public biotechnology company, from July 2012 until February 2019, which he joined in connection with an investment by Sofinnova, and Avedro, Inc. (NASDAQ: AVDR), a commercial-stage ophthalmic medical technology company, from April 2017 until November 2019. Dr. Kong also previously served on the Board of Melinta Therapeutics (NASDAQ: CEMP), a pharmaceutical company formerly known as Cempra Pharmaceuticals, from September 2006 until June 2019. Dr. Kong also sits on the Duke University Medical Center Board of Visitors.

Peter M. Neupert

61. Defendant Peter M. Neupert ("Neupert") has served as a director since January 2013. Neupert is the chairperson of the Company's Nominating and

Corporate Governance Committee and a member of the Audit Committee.

62. According to the Company's 2020 Proxy Statement, in 2019 Neupert received total compensation of $327,366. This included $147,500 in cash and $179,866 in stock awards.

63. According to the Company's 2020 Proxy Statement, Neupert beneficially owns 9,996 shares of the Company's common stock.

64. The Company's 2020 Proxy Statement stated the following about Defendant Neupert:

> Peter M. Neupert has served as a director of the Company since January 2013. Mr. Neupert was an Operating Partner at Health Evolution Partners, a health only, middle market private equity firm, from January 2012 until June 2015. Prior to that, Mr. Neupert served as Corporate Vice President of the Microsoft Health Solutions Group from its formation in 2005 to January 2012. Mr. Neupert served on the President's Information Technology Advisory Committee (PITAC), co-chairing the Health Information Technology Subcommittee and helping to drive the "Revolutionizing Health Care Through Information Technology" report, published in June 2004. Mr. Neupert served as the founding President and Chief Executive Officer of drugstore.com from 1998 to 2001 and as Chairman of the board of directors through September 2004. Mr. Neupert has served as a director of Adaptive Biotechnologies Corporation (NASDAQ: ADPT) since December 2013 and currently serves as the Lead Independent Director. He is also a Director of Clinithink Ltd. and Navigating Cancer Inc. He served on the Board of Directors of Quality Systems, Inc., now known as NextGen Healthcare, Inc. (NASDAQ: NXGN) from August 2013 to January 2014 and Freedom Innovations LLC from May 2013 to April 2016. He serves as a trustee for the Fred Hutchinson Cancer Research Center and was an active member of the Institute of Medicine's Roundtable on Value & Science-Driven Healthcare from 2007 to 2011. Mr. Neupert brings to the Board experience as a recognized expert in health information technology and perspective on how to grow shareholder value leveraging business strategies with technology. Mr. Neupert is an audit committee financial expert as a result of his experience, including his

> experience as CEO and Chairman of drugstore.com. Mr. Neupert serves as the Board's Lead Independent Director and brings a deep understanding of the role of the Board and its oversight of corporate governance and business strategy.

Richelle P. Parham

65. Defendant Richelle P. Parham ("Parham") has served as a director since February 2016. Parham is a member of the Company's Audit Committee and Nominating and Corporate Governance Committee.

66. According to the Company's 2020 Proxy Statement, in 2019 Parham received total compensation of $289,866. This included $110,000 in cash and $179,866 in stock awards.

67. According to the Company's 2020 Proxy Statement, Parham beneficially owns 5,088 shares of the Company's common stock.

68. The Company's 2020 Proxy Statement stated the following about Defendant Parham:

> Richelle Parham has served as a director of the Company since February 8, 2016. In October 2019, Ms. Parham became a Managing Director of WestRiver Group, which is a collaboration of leading investment firms that provides integrated capital solutions to the global innovation economy with investments focused on technology, life sciences, energy, and experiential sectors. She is currently a Strategic Advisor at Camden Partners, a private equity firm, where she previously served as a General Partner from October 2016 to October 2019. Prior to Camden Partners, Ms. Parham served as Vice President, Chief Marketing Officer of eBay from November 2010 to March 2015. Ms. Parham was responsible, globally, for eBay brand strategy and brand marketing, to reach 108+ million active eBay users, Internet marketing and for customer relationship management. Prior to joining

> eBay, Ms. Parham served as head of Global Marketing Innovation and Initiatives and head of Global Marketing Services at Visa, Inc. from 2008 to 2010. Her experience also includes 13 years at Digitas, Inc., a leading marketing agency, where she held a variety of senior leadership roles, including senior vice president and general manager of the agency's Chicago office. An advocate of empowering female leaders through STEM programs, Ms. Parham is on the advisory board for Girls Who Code. Ms. Parham has served as a Director of Best Buy Co., Inc. (NYSE: BBY) and e.l.f. Beauty, Inc. (NYSE: ELF) since March 16, 2018. She served on the board of directors for Scripps Network Interactive Inc. (NYSE:SNI) from 2012 to March 2018, when Scripps Network was acquired by Discovery Communications. Ms. Parham holds double Bachelor of Science degrees in business administration and design arts from Drexel University. She became a member of the Drexel University board of trustees in 2014.

R. Sanders Williams, M.D.

69. R. Sanders Williams, M.D. ("Williams") has served as a director since May 2007. Williams is chairperson of the Company's Quality and Compliance Committee and a member of the Audit Committee.

70. According to the Company's 2020 Proxy Statement, in 2019 Williams received total compensation of $304,866. This included $125,000 in cash and $179,866 in stock awards.

71. According to the Company's 2020 Proxy Statement, Williams beneficially owns 7,695 shares of the Company's common stock.

72. The Company's 2020 Proxy Statement stated the following about Defendant Williams:

> Dr. R. Sanders Williams has served as a director of the Company since May 16, 2007. Dr. Williams has served as President Emeritus of The J.

David Gladstone Institutes since January 1, 2018. Prior to this appointment, he was president of The J. David Gladstone Institutes since November 2009, and he served as Chief Executive Officer of The J. David Gladstone Foundation until December 31, 2018. Dr. Williams also currently is Professor of Medicine at the University of California San Francisco, Professor of Medicine at Duke University, and Senior Advisor for science and technology, Duke University. Dr. Williams served Duke University between 2001 and 2010 as Dean of the School of Medicine, Senior Vice Chancellor, Senior Advisor for International Strategy, and founding Dean of the Duke-NUS Graduate Medical School Singapore. He has served previously as President of the Association of University Cardiologists, Chairman of the Research Committee of the American Heart Association, on the editorial boards of leading biomedical journals, on the Advisory Committee to the Director of the National Institutes of Health and on the board of external advisors of the National Heart, Lung and Blood Institute. Dr. Williams was a director of Bristol-Meyers Squibb Company (NYSE: BMS) from 2006 until May 2013 and has been a director of Amgen, Inc. (NASDAQ: AMGN) since October 2014. Dr. Williams is a member of the National Academy of Medicine, and a Fellow of the American Association for the Advancement of Science.

FIDUCIARY DUTIES OF THE INDIVIDUAL DEFENDANTS

73. By reason of their positions as officers, directors, and/or fiduciaries of LabCorp and because of their ability to control the business and corporate affairs of the Company, the Individual Defendants owed LabCorp and its shareholders fiduciary obligations of loyalty, care and good faith, and were and are required to use their utmost ability to control and manage the Company in a fair, just, honest, and equitable manner. The Individual Defendants were and are required to act in furtherance of the best interests of LabCorp and its shareholders to benefit all shareholders equally and not in furtherance of their personal interest or benefit.

74. Each director and officer of the Company owes to LabCorp and its shareholders the fiduciary duty to exercise good faith and diligence in the administration of the Company's affairs and in the use and preservation of its property and assets, and the highest obligations of fair dealing.

75. The Individual Defendants, because of their positions of control and authority as directors and/or officers of LabCorp, were able to and did, directly and/or indirectly, exercise control over the wrongful acts complained of herein, as well as the contents of various public statements issued by the Company. Due to their positions with LabCorp, each of the Individual Defendants had knowledge of material non-public information regarding the Company.

76. To discharge their duties, the Individual Defendants were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the Company. By virtue of such duties, the officers and directors of LabCorp were required to, among other things:

a. Exercise good faith to ensure that the affairs of the Company were conducted in an efficient, business-like manner to make it possible to provide the highest quality performance of their business;

b. Exercise good faith to ensure that the Company was operating in a diligent, honest and prudent manner and complied with all applicable federal, state and foreign laws, rules, regulations and

requirements, and all contractual obligations, including acting only within the scope of its legal authority;

c. Exercise good faith in supervising the preparation, filing and/or dissemination of financial statements, press releases, audits, reports or other information required by law, and in examining and evaluating any reports or examinations, audits, or other financial information concerning the financial condition of the Company;

d. Refrain from unduly benefiting themselves and other Company insiders at the expense of the Company; and

e. When put on notice of problems with the Company's business practices and operations, exercise good faith in taking appropriate action to correct the misconduct and prevent its recurrence.

77. Moreover, LabCorp's board of directors adopted a Code of Conduct and Ethics ("Code") which is applicable "to all LabCorp employees, officers, directors, vendors, and contractors . . . ." The Code states the following, in part:

> Employees, officers, and directors must maintain the confidentiality of information entrusted to them by LabCorp or its customers, except when LabCorp's Global General Counsel or Law Department authorizes disclosure or such disclosure is required by law. **Confidential information** includes all non-public information that might be of use to competitors or harmful to LabCorp or its customers if disclosed. It also **includes information that suppliers and customers have entrusted to us.** Confidential information may also include information regarding LabCorp's competitors. The obligation to preserve confidential information continues even after employment

with LabCorp ends.

* * *

> The Board of Directors, through the Audit and Quality and Compliance Committees, will help support the proper administration of this Code. The Audit Committee is responsible for monitoring compliance from a financial point of view and the **Quality and Compliance Committee is responsible for monitoring compliance from a health care regulatory perspective.** The Audit and Quality and Compliance Committees will be responsible for the annual review of the compliance procedures in place to implement this Code and will recommend clarifications or necessary changes to this Code to the full Board for approval.

(Emphasis added).

78. The Company also has an Audit Committee, Compensation Committee, Quality and Compliance Committee, and a Nominating and Corporate Governance Committee. Each committee has a respective charter to govern the committee members' duties and responsibilities.

79. The Audit Committee Charter states the following, in part:

> The Audit Committee is appointed by the Board to be directly responsible for (a) the selection, appointment, compensation, retention and oversight of the work of any registered public accounting firm employed by the Company, (b) to assist in Board oversight of (1) the integrity of the financial statements of the Company; (2) the compliance by the Company with legal and regulatory requirements; (3) the qualifications and independence of the Company's independent auditors; and (4) the performance of the Company's internal audit function and independent auditors, and (c) the preparation of the disclosure required by Item 407(d)(3)(i) of Regulation S-K.

* * *

> The Audit Committee shall meet periodically with management, internal audit staff, and the independent auditors to review and discuss the Company's major financial risk exposures, including any critical audit matters, and the steps management has taken to monitor and control such exposures, including with respect to risk assessment and risk management. The Audit Committee shall also review and evaluate the Company's processes for identifying and assessing key financial statement risk areas and for formulating and implementing steps to address such risk areas.
>
> * * *
>
> **The Audit Committee shall regularly review the Company's cybersecurity and other information technology risks, controls and procedures, including the Company's plans to mitigate cybersecurity risks and to respond to data breaches. The Audit Committee shall also review with management any specific cybersecurity issues that could affect the adequacy of the Company's internal controls.**

(Emphasis added).

80. Additionally, the Company's 2020 Proxy Statement states that the Audit Committee is responsible for "review[ing] the Company's cybersecurity and other information technology risks, controls and procedures, including plans to mitigate cybersecurity risks and respond to data breaches." The 2020 Proxy Statement also states the following:

> The Audit Committee regularly reviews the Company's cybersecurity and other information technology risks, controls and procedures, including plans to mitigate cybersecurity risks and respond to data breaches. **The Audit Committee receives reports at its regularly scheduled meetings from the Chief Information Security Officer and the Chief Information Officer on, among other things, the Company's cyber risks and threats, the status of projects to strengthen the Company's information security systems,**

assessments of the Company's security program and the emerging threat landscape. In addition, the full Board receives briefings from the Chief Information Security Officer and the Chief Information Officer twice per year.

(Emphasis added).

81. The Compensation Committee Charter states, in part:

The Compensation Committee (the "Compensation Committee") is appointed by the Board (i) to discharge the Board's responsibilities relating to the oversight of the Company's compensation and benefits policies generally, (ii) to evaluate the performance of and oversee and set compensation for the Company's Chief Executive Officer ("CEO"), the Company's Section 16 Officers (which as used in this charter includes officers within the meaning of Section 16 of the Securities Exchange Act of 1934 (the "Act") and the Company's "executive officers" within the meaning of Rule 3b-7 as promulgated under the Act), and (iii) to consider, recommend, administer and implement the Company's incentive-compensation plans and equity-based plans.

The Compensation Committee is also responsible for (i) overseeing and assisting the Company in preparing the Compensation Discussion & Analysis ("CD&A") for inclusion in the Company's proxy statement and/or annual report on Form 10-K, (ii) providing for inclusion in the Company's proxy statement a description of the processes and procedures for the consideration and determination of executive and director compensation, and (iii) preparing and submitting for inclusion in the Company's proxy statement and/or annual report on Form 10-K a Compensation Committee Report, each as more fully described below and in accordance with applicable rules and regulations.

82. The Quality and Compliance Committee Charter states, in part:

The Quality and Compliance Committee is appointed by the Board to assist the Board in (1) carrying out its oversight responsibility with respect to quality and compliance issues and attendant risks and (2) to oversee management's efforts to adopt and implement policies and procedures that require the Company and its employees to deliver high quality services, to act in compliance with high ethical and legal

> standards, and to be compliant with applicable operational, health, safety, quality, environmental, and regulatory requirements and best practices (see the Audit Committee Charter regarding financial control, audit, and accounting matters).

83. The Nominating and Corporate Governance Committee Charter states, in part:

> The Nominating and Corporate Governance Committee is appointed by the Board (1) to assist the Board by identifying individuals qualified to become Board members, consistent with criteria approved by the Board and by recommending to the Board the director nominees for the next annual meeting of stockholders and otherwise when necessary; (2) to develop and recommend to the Board a set of corporate governance guidelines applicable to the Company and appropriate amendments thereto; (3) to lead the Board in its annual review of the performance of the Board and management; and (4) to oversee, and advise the Board with respect to, the Company's corporate governance matters, including Board and committee structure and composition and the Company's corporate governance policies and practices.

84. Each Individual Defendant, by virtue of his position as a director and/or officer, owed to the Company and its shareholders the fiduciary duties of loyalty, care and good faith, and the exercise of due care and diligence in the management and administration of the affairs of the Company, as well as in the use and preservation of its property and assets. The conduct of the Individual Defendants complained of herein involves a knowing and culpable violation of their obligations as directors and/or officers of LabCorp, the absence of good faith on their part and a reckless disregard for their duties to the Company and its shareholders that the Individual Defendants were aware or had reason to be, were reckless in not being, or should have been aware posed a risk of serious injury to the Company.

85. The Individual Defendants breached their duties of loyalty, care and good faith by: (i) failing to implement and enforce a system of effective internal controls and procedures to protect patients' PII and PHI; (ii) failing to exercise their oversight duties by not monitoring the Company's compliance with Company procedures and federal and state regulations; (iii) providing PII and PHI of patients to a business associate with deficient cybersecurity and breach detection; (iv) failing to ensure that the Company, as well as its business associates, utilized proper cybersecurity safeguards to adequately secure the PII and PHI; (v) failing to have a sufficient incident response plan to immediately respond to the Data Breaches; (vi) consciously disregarding, delaying, and failing to ensure that the Company notified all potentially affected individuals and entities in a timely manner upon discovering the Data Breaches; (vii) failing to make adequate public disclosure of the Data Breaches; and (viii) allowing the Company to violate state and federal laws and regulations.

SUBSTANTIVE ALEGATIONS

Background

86. LabCorp 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.

87. The Company is one of the world's leading providers of medical

diagnostic testing services for patient care. For these and other services, LabCorp generated revenues of approximately $11.3 billion in 2018.

88. LabCorp offers a variety of clinical laboratory testing services to patients following a referral from a physician. According to the Company's annual report on Form 10-K for the period ended December 31, 2018, filed with the SEC on February 28, 2019 (the "2018 Form 10-K"), LabCorp processes "more than 2.5 million patient specimens each week and has laboratory locations throughout the U.S. and other countries, including Canada."

89. LabCorp operates a network of "Patient Service Centers" ("PSCs") throughout the U.S., at which it performs specimen collection services for patients. Its PSC staff, generally phlebotomists, collect specimens for testing as requested by the ordering physician. Additionally, according to the 2018 Form 10-K, "[a] significant portion of patient specimens are collected by [healthcare providers'] staff at its office or facility, or in some cases, by a [LabCorp] phlebotomist who has been placed in the [healthcare providers'] location for the specific purpose of collecting and processing specimens to be tested by [LabCorp]."

90. For appointments at its PSCs, LabCorp requires patients to bring with them and provide to LabCorp a LabCorp test request form or prescription from the healthcare professional requesting the laboratory testing; a current insurance identification card (Medicare, private insurance or HMO/PPO); a photo ID; and a

health spending account card, credit card, or debit card.

91. LabCorp promises that its "staff will make the specimen collection process as safe, quick, and comfortable as possible **while safeguarding your dignity and privacy**."[2] (Emphasis added).

92. LabCorp charges for the laboratory services it provides to patients. If the patient does not have insurance, or if the insurance does not cover the clinical laboratory testing services, the patient is responsible for paying for the full amount of the services performed.

93. LabCorp generates bills for its patients. Accounts receivable are then monitored by LabCorp billing personnel and follow-up activities are conducted as necessary.

94. LabCorp refers unpaid bills to a collection agency. AMCA is an external collection agency LabCorp utilized to collect unpaid bills. LabCorp has referred more than 10.2 million patients to AMCA. AMCA is a "business associate" of LabCorp under The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). According to the U.S. Department of Health & Human Services ("HHS"):

> A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business

[2] https://www.labcorp.com/labs-and-appointments/what-to-expect

> associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.
>
> Business associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial. See the definition of "business associate" at 45 CFR 160.103.[3]

95. LabCorp provided AMCA with PII and PHI regarding LabCorp's patients in order to facilitate the bill-collection process. The PII and PHI was stored in AMCA systems.

96. The PII and PHI LabCorp provided AMCA included personal and medical information, such as the first and last name, date of birth, address, telephone number, date of service, service provider, and account balance information.

97. AMCA collects and maintains the information provided by LabCorp in its own computer systems. Additionally, AMCA obtains LabCorp patients' PII and PHI when AMCA seeks to collect payments on LabCorp's behalf. This information

[3] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.

includes financial information, such as credit card or bank account information. Upon information and belief, AMCA stored this information on AMCA computer systems.

98. In U.S. Bankruptcy Court in the Southern District of New York, AMCA has admitted that its "business, by its very nature, requires it to collect and maintain data transmitted to it by its clients [such as LabCorp] that includes personally identifiable information about third-party debtors that could include names, home addresses, social security numbers, bank account information for consumers choosing to pay online by check and, for consumers choosing to pay their outstanding balances by credit card, credit card information." AMCA has also admitted that this "information might also include dates of birth and certain medical information related to any laboratory tests for which payment is sought."[4]

A Large Number of Compromised Payment Cards Were Identified on the Dark Web

99. On February 28, 2019, analysts from cybersecurity firm Gemini identified a large number of compromised payment cards on the dark web[5]

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

[5] The dark web is generally described as "the portion of the Internet that is intentionally hidden from search engines, uses masked IP addresses, and is accessible only with a special web browser: part of the deep web." https://www.dictionary.com/browse/dark-web?s=t.

containing PII and PHI, such as dates of birth ("DOBs"), Social Security numbers ("SSNs"), and physical addresses.[6]

100. An analysis conducted by Gemini indicated that the information was likely stolen from AMCA's online portal, and several financial institutions confirmed the connection between the compromised payment card data and the AMCA Incident.[7]

101. During Gemini's initial analysis, Gemini believed that the AMCA Incident caused roughly 10,000 individuals' PPI to be exposed; however, further analysis revealed that the number of victims exceeded 200,000, and records are continually being added to the dark web.

102. Through the AMCA Incident, more than 10.2 million LabCorp patients were affected by the First Breach, which is the second-largest breach (behind only the breach of Quest Diagnostics Inc. ("Quest") patients' data) reported to HHS in 2019.[8] LabCorp's data breach was also the fourth-largest to be reported since HHS's

---

[6] Gemini Advisory, *AMCA Breach May Be Largest Medical Breach in 2019* (June 4, 2019), https://geminiadvisory.io/amca-largest-medical-breach/.

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

[8] U.S. Dep't of Health and Human Services, Office for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Apr. 17, 2020); *see also* HIPAA Journal, *August 2019 Healthcare Data Breach Report* (Sept. 23, 2019), https://www.hipaajournal.com/august-2019-healthcare-data-breach-report/.

Office for Civil Rights launched its breach portal in 2010.[9]

103. Gemini noted that the top ten (10) states where patients were affected included: California, Texas, Florida, Georgia, Tennessee, Virginia, Maryland, Pennsylvania, New Jersey, and New York.

104. According to Gemini, on March 1, 2019, Gemini Advisory attempted to notify AMCA, but as Gemini reported to DataBreaches.net, "[Gemini] did not get any response to phone messages they left." Failing to obtain any response from AMCA, Gemini "promptly contacted federal law enforcement, who reportedly followed up by contacting AMCA."[10]

105. On May 10, 2019, DataBreaches.net published an article announcing the AMCA Incident, which heavily relied on information discovered by Gemini (the "DataBreaches.net Article").[11] In a statement to DataBreaches.net describing why the AMCA Incident posed greater risks to patients than other payment card breaches, Stas Alforov, Gemini's Director of Research, stated the following, in relevant part:

> In a medical breach, personal debit and credit cards are not the only thing at stake. Health Savings Accounts (HSAs) are often tied to specialized debit cards that are used to make medical-based payments but can also be used for regular purchases at the cost of a severe tax

[9] Modern Healthcare, *July-reported healthcare breaches exposed 22 million people's data* (Aug. 9, 2019), https://www.modernhealthcare.com/cybersecurity/july-reported-healthcare-breaches-exposed-22-million-peoples-data.
[10] DataBreaches.net, *American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory* (May 10, 2019), https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/.
[11] *Id.*

penalty.

> Account holders often only periodically use HSAs due to the incentives for accumulating funds that can later be withdrawn without any penalties during retirement, meaning that they are likely not as closely monitored for any daily unauthorized activities. Thus, they make easier targets for criminal actors who attempt to monetize the compromised data from medical breaches such as AMCA's.

106. The DataBreaches.net Article revealed that AMCA's payment portal was disabled by April 8, 2019 at the latest, and remained unavailable until May 2019, when it became operational again. For nearly a month, LabCorp did not realize AMCA's payment portal was inoperable. The lack of operation of AMCA's payment portal and meaningful oversight and investigation by the Individual Defendants directly impacted collection efforts performed on behalf of LabCorp. Additionally, the DataBreaches.net Article reported that despite being inoperable, AMCA failed to otherwise disclose the AMCA Incident.

107. On May 14, 2019, AMCA notified LabCorp of the AMCA Incident. In response to AMCA's report of the First Breach, LabCorp later claimed it informed AMCA that the Company would cease sending new collection requests to AMCA and told AMCA to stop work on any pending collection requests involving LabCorp patients.[12]

108. Even after receiving direct notice from AMCA, LabCorp did not make

[12] LabCorp, *Notice Regarding AMCA Security Incident* (July 13, 2019), https://www.labcorp.com/AMCA-data-security-incident.

immediate public disclosure.

Quest and Optum360, LLC ("Optum360") Disclose the First Breach

109. On June 3, 2019, Quest filed a current report on Form 8-K with the SEC (the "Quest 8-K") announcing that AMCA had notified Quest and Optum360 of the AMCA Incident. The Quest 8-K stated the following, in relevant part:

> On May 14, 2019, American Medical Collection Agency (AMCA), a billing collections vendor, notified Quest Diagnostics Incorporated ("Quest Diagnostics") and Optum360 LLC, Quest Diagnostics' revenue cycle management provider, of potential unauthorized activity on AMCA's web payment page. Quest Diagnostics and Optum360 promptly sought information from AMCA about the incident, including what, if any, information was subject to unauthorized access.
>
> Although Quest Diagnostics and Optum360 have not yet received detailed or complete information from AMCA about the incident, AMCA has informed Quest Diagnostics and Optum360 that:
>
> - Between August 1, 2018 and March 30, 2019 an unauthorized user had access to AMCA's system that contained information that AMCA had received from various entities, including Quest Diagnostics, and information that AMCA collected itself;
>
> - The information on AMCA's affected system included financial information (*e.g.,* credit card numbers and bank account information), medical information and other personal information (*e.g.*, Social Security Numbers);
>
> - As of May 31, 2019, AMCA believes that the number of Quest Diagnostics patients whose information was contained on AMCA's affected system was approximately 11.9 million people; and
>
> - AMCA has been in contact with law enforcement regarding the incident.

> Quest Diagnostics has not been able to verify the accuracy of the information received from AMCA.
>
> Quest Diagnostics' laboratory test results were not provided to AMCA and were therefore not impacted by this incident.
>
> In response to this incident, Quest Diagnostics has:
>
> - Suspended sending collection requests to AMCA;
> - Provided notifications to affected health plans and will ensure that notification is provided to regulators and others as required by federal and state law; and
> - Been working and will continue to work diligently, along with Optum360, AMCA and outside security experts, to investigate the AMCA data security incident and its potential impact on Quest Diagnostics and its patients.

Multiple Media Outlets Publicize the First Breach

110. Shortly after Quest and Optum360 disclosed the AMCA Incident, multiple media outlets publicized the AMCA Incident. In an article by *CNET*[13] published on June 3, 2019, the firm representing AMCA stated that it was investigating the "data incident" and provided the following statement on behalf of 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

[13] Carrie Mihalcik, *Quest Diagnostics says data on nearly 12M patients exposed by breach*, CNET (June 3, 2019), https://www.cnet.com/news/quest-diagnostics-says-nearly-12m-patients-exposed-by-data-breach/.

> 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.

111. The AMCA Incident received wide ranging media attention with multiple national news outlets publishing articles on June 3, 2019.

LabCorp Discloses the First Breach

112. LabCorp waited until the next day, June 4, 2019, to make its first public disclosure of the First Breach. Prior to this disclosure, the Individual Defendants ignored the First Breach until the media attention and disclosure by Quest brought a significant amount of attention to the First Breach. Had Quest decided against disclosing the First Breach, LabCorp and the Individual Defendants could have continued to withhold details of the First Breach from the public.

113. LabCorp failed to timely disclose the First Breach despite that the Company knew or had reason to know, were reckless in not knowing, or should have known about the First Breach no later than March 2019. As aforementioned, Gemini identified the AMCA Incident in February of 2019, attempted to contact AMCA on March 1, 2019, and subsequently notified federal authorities in early March 2019.

114. On June 4, 2019, LabCorp filed a current report on Form 8K with the SEC ("June 2019 8-K") indicating that LabCorp was aware that a contractor utilized by the Company had unauthorized activity on its website. Specifically, the June 2019 8-K stated, in relevant part:

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 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.

(Emphasis added).

115. As indicated in the June 2019 8-K, LabCorp only announced the First Breach in the SEC filing in order to respond "to questions it has received[.]"

116. Following the announcement of the First Breach, on June 5, 2019, United States Senators Robert Menendez and Cory A. Booker sent a letter to LabCorp requesting more information about the First Breach, including LabCorp's data security policies and procedures and the steps LabCorp has taken since learning of the First Breach.[14] Additionally, the Senators note that LabCorp has historically failed to protect patient PII and PHI. Specifically:

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

(Emphasis added).

117. Two days later, Connecticut Attorney General William Tong ("Connecticut AG") and Illinois Attorney General Kwame Raoul ("Illinois AG")

[14] Letter from Sens. Robert Menendez and Cory A. Booker to Sandra D. van der Vaart 1 (June 5, 2019), https://www.menendez.senate.gov/imo/media/doc/06.05.19%20LabCorp%20Letter.pdf.

announced that they had opened an investigation into the AMCA Incident and had sent letters to AMCA, Quest, and LabCorp seeking more information from the companies.[15]

118. Although LabCorp's June 2019 8-K stated that "AMCA has advised LabCorp that Social Security Numbers and insurance identification information are not stored or maintained for LabCorp consumers[,]" LabCorp subsequently disclosed in a Form 10-Q filed with the SEC on August 8, 2019 (the "August 2019 10-Q") that Social Security numbers and health insurance information may have been taken as well. [redacted]

119. LabCorp's August 2019 10-Q stated the following:

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

[15] Conn. Office of the Attorney General, *Connecticut And Illinois Open Investigation Into Quest Diagnostics, Labcorp Data Breach* (June 7, 2019), https://portal.ct.gov/AG/Press-Releases/2019-Press-Releases/CT-AND-IL-OPEN-INVESTIGATION-INTO-QUEST-AND-LABCORP-DATA-BREACH.

(Emphasis added).

120. On or about July 13, 2019, LabCorp disclosed to the Office for Civil Rights that 10,251,784 individuals have been affected by the First Breach.[16] LabCorp did not disclose the extent of the First Breach in either the August 2019 10-Q or on the Company's website.

The Individual Defendants Failed to Exercise Due Care in Contracting With AMCA

121. The Individual Defendants failed to exercise due care in protecting patients' PII and PHI by contracting with AMCA to handle the Company's debt collections.

122. AMCA's bankruptcy filings indicate how thinly capitalized the company was and how insufficient its information technology ("IT") department and infrastructure were. Public reporting has highlighted that AMCA was not a reputable business associate – let alone an associate to be trusted with LabCorp's patient information.

123. Specifically, AMCA's bankruptcy filings admit that it had less than $4 million in liquidity and its owner had to take a secured loan from his own personal funds simply to mail notices to those impacted by the AMCA Incident. The

[16] U.S. Dep't of Health and Human Services, Office for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Apr. 17, 2020).

Individual Defendants should not have permitted LabCorp to contract with an entity that did not even have the means to mail notices to people without having to file for bankruptcy.

124. The length of time between the breach and AMCA's claimed discovery of the breach indicates that AMCA's systems to detect intrusion, detect unusual activity, and log and report such events were inadequate and did not meet industry standards. For example, according to technology-security company FireEye, the median dwell time from when a breach occurs to when it is detected was 30 days in 2019.[17] The fact that it took AMCA 242 days to detect the AMCA Incident (and LabCorp never discovered the First Breach on its own), nearly 8 times the median time for detection in 2019, demonstrates AMCA's failure to employ reasonable, industry-standard data security practices to safeguard LabCorp's patients' PII and PHI. AMCA's data security deficiencies would have been readily apparent to the Individual Defendants had the Individual Defendants themselves, or LabCorp employees under the direction of the Individual Defendants, adequately investigated AMCA's capabilities (or lack thereof).

125. AMCA's inability to detect the AMCA Incident, when Gemini was apparently able to do so with ease, is further evidence of the fact that the Individual

[17] Dwell time is "calculated as the number of days an attacker is present in a victim network before they are detected." *M-Trends 2020: FireEye Mandiant Services Special Report*, https://content.fireeye.com/m-trends (the "FireEye Report").

Defendants contracted with a company that employed inadequate data security practices, and that the Individual Defendants and LabCorp each failed in their independent obligations to ensure that its HIPAA business associate employed reasonable and industry-standard data security measures.

126. The FireEye Report indicates that in 2018, the median amount of time that it took a third party to detect a data breach was four times the median time for internal detection. Here, third-party Gemini detected the AMCA Incident, and it's unknown when and if AMCA would have detected the breach.

127. Simple and standard ways to minimize exposure to a data breach include limiting the type and amount of information provided to business associates and routinely destroying or archiving inactive PII and PHI so that it cannot be accessed through online channels. Access to the 10.2 million LabCorp patient records through AMCA's online portal should not have been possible had the Individual Defendants ensured AMCA maintained appropriate protections. The sheer number of records exposed suggests that AMCA was not destroying or archiving inactive records. Again, the Individual Defendants and/or LabCorp would have discovered this had it exercised adequate oversight over its business associates and audited the data security protocols utilized by AMCA.

128. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit

payment card data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). AMCA was not encrypting payment card information according to minimum industry standards established in PCI DSS. The Individual Defendants knew or had reason to know, were reckless in not knowing, or should have known that AMCA was not complying with PCI DSS.

129. 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 . . . is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[18]

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

131. The Individual Defendants had an obligation to exercise oversight over

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

AMCA in a manner that would include immediate knowledge of any data security incidents experienced by AMCA that could affect LabCorp's patients. For example, AMCA pointed to the fact that it learned of the unauthorized access in March 2019 through a series of CPP notices suggesting that a "disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges."

132. LabCorp claims it did not learn of the unauthorized access until months later in May 2019. This gap in time demonstrates that LabCorp and the Individual Defendants not only failed to oversee AMCA as a business associate, but also that the Individual Defendants failed to enforce contractual provisions designed to protect patients' PII and PHI.

The Individual Defendants and LabCorp Failed to Provide Proper Notice of the Data Breach in Violation of Numerous State and Federal Laws

133. Although LabCorp received direct notice of the First Breach on May 14, 2019 (and knew or had reason to know, were reckless in not knowing, or should have known months earlier), it took LabCorp twenty-one (21) days to publicly acknowledge the First Breach and months longer to provide notice to impacted patients (and similarly failed to provide adequate and timely notice of the Second Breach, discussed below).

134. On June 4, 2019, LabCorp publicly acknowledged the First Breach and indicated that it would be "working closely with AMCA to obtain more information

and to take additional steps as may be appropriate once more is known about the AMCA Incident."

135. However, rather than sending notice directly to its patients, LabCorp disclosed in the June 2019 8-K that the Company was relying on AMCA to mail notices to LabCorp patients with PII and/or PHI on AMCA's system. The notice provided by AMCA was deficient in several respects.

136. AMCA's notices failed to indicate to LabCorp's patients that it was LabCorp who had given their information to AMCA. Thus, many affected individuals were left to guess why AMCA had their PII and PHI in the first instance.

137. The notices further failed to inform LabCorp's patients exactly what information was breached, thus preventing them from taking independent remedial measures to protect themselves.

138. Strikingly, LabCorp wholly relied upon AMCA, while AMCA was seeking bankruptcy protection, to adequately advise and assist its patients through the First Breach. LabCorp failed to accept responsibility and adequately respond to the First Breach. Instead, a multibillion-dollar business, LabCorp, relied on undercapitalized and unsophisticated AMCA to send out the breach notices.

139. Through the June 2019 8-K, LabCorp notes that *AMCA* will attempt to send notices regarding the First Breach to affected LabCorp patients; however, the June 2019 8-K does not indicate that LabCorp will be sending notices, or otherwise

informing patients:

> 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.

140. Notably, the notice above appears to be limited to "consumers whose credit card or bank account information may have been accessed." Nevertheless, the estimated numbers below suggest that a substantial portion of affected LabCorp patients, who had other forms of information exposed, would not receive a notice from AMCA regarding the breach.

141. Additionally, as later estimated, nearly 10.2 million LabCorp patients' PII and/or PHI was exposed; nonetheless, LabCorp and the Individual Defendants were satisfied with or consciously ignored the fact that AMCA intended to provide notice to only 200,000 LabCorp patients. This represents less than 2% of affected LabCorp patients receiving notice from AMCA. The Company and the Individual Defendants knew or had reason to know, were reckless in not knowing, or should have known that notice provided to such a limited customer base was deficient and/or was likely to violate established notice laws and regulations.

142. LabCorp did not even immediately receive a list of affected LabCorp consumers. According to the June 2019 8-K, LabCorp still had not obtained a list of affected LabCorp consumers: "AMCA has not yet provided LabCorp a list of the affected LabCorp consumers or more specific information about them."

143. It was not until July 13, 2019, almost four (4) months after AMCA received notice about the First Breach and more than a month after LabCorp's first public statement, that LabCorp put detailed information on its own website regarding the First Breach. But even this more detailed notice was deficient in many respects:

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

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

c. Third, LabCorp acknowledges that it may have out-of-date contact information for some of its patients. However, LabCorp provided no means for these patients to obtain information about whether they had been breached and to access credit monitoring. For example, LabCorp's website does not have any information that its patients can use to determine whether their information was part of the First

Breach.

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

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

144. LabCorp purportedly mailed letters to patients potentially affected by the First Breach on or around July 13, 2019. [redacted] There is, however, no indication that LabCorp received a list of all affected LabCorp patients or whether the Company and Individual Defendants compiled, or attempted to compile, a complete list of patients affected by the First Breach.

145. [redacted]

[redacted]

146. Additionally, LabCorp provided notice and a description of the First Breach to state attorneys general, United States Senators, federal and state agencies, some of which were only provided after LabCorp received requests for information. Many of these disclosures violated state statutes implemented to protect customers from data/security breaches and prevent identity theft and contained incorrect information. Many states codified statutes and regulations relating to the timing of such notice in an effort to curb the harm of a data breach. [redacted]

147. On June 14, 2019, LabCorp directly responded to an information request sent to the Company by United States Senator Robert Mendendez and United State Senator Cory A. Booker on June 5, 2019. (LCA000079–80). [redacted] However, as aforementioned, AMCA was well aware of the AMCA Incident prior to May 14,

2019, and independent securities firms and financial organizations learned of the AMCA Incident in February 2019. As such, LabCorp and the Individual Defendants failed to sufficiently enforce contractual provisions designed to protect LabCorp patients from incidents like the First Breach. Moreover, this response demonstrates LabCorp's wholly inadequate oversight of its business associate, AMCA.

148. [redacted]

a. [redacted]

b. [redacted]

c. [redacted]

d. [redacted]

[redacted]

e. [redacted]

f. [redacted]

g. [redacted]

h. [redacted]

i. [redacted]

j. [redacted]

k. [redacted]

[redacted]

l. [redacted]

m. [redacted]

n. [redacted]

o. [redacted]

p. [redacted]

q. [redacted]

r. [redacted]

s. [redacted]

[redacted]

149. [redacted]

[redacted]

a. [redacted]

b. [redacted]

150. [redacted]

[redacted]

[redacted]

151. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

152. As aforementioned and as disclosed in the multiple letters to state attorneys general and the online disclosure submissions, LabCorp claims the Company learned of the First Breach on May 14, 2019. The information provided to a majority of the states and agencies by LabCorp indicates that LabCorp began providing notice to affected patients on July 13, 2018.[19]

153. Numerous states provide that notification to state attorneys general and

[19] The notice date provided by LabCorp pre-dates the First Breach; as such, upon information and belief, Plaintiff assumes, for this allegation, that the Company began providing notice on July 13, 2019.

customers affected by a data/security breach "shall be made as expeditiously as possible and without unreasonable delay[.]"[20] Additionally, certain states impose time limits on providing notifications, such as within thirty (30)[21], forty-five (45)[22], sixty (60)[23], or ninety (90)[24] days of discovery of the breach.

154. [redacted] LabCorp waited a minimum of sixty (60) days, between at least May 14, 2019 through July 13, 2019, to notify affected customers. Moreover, LabCorp should have known about the First Breach no later than March 2019, which would lengthen the delayed notification to nearly five (5) months.

155. Based on the disclosure letters and online reports, LabCorp violated state statutes relating to timely notification by exceeding the statutory notice period of thirty (30) days in Florida, which provides that disclosure "shall be made as expeditiously as practicable and without unreasonable delay . . . but no later than 30 days after the determination of a breach or reason to believe a breach occurred . . . ."[25]

156. LabCorp also violated the statutory notice period in Colorado, which

[20] *See, e.g.*, Ala. Code § 8-38-1 *et. seq.*
[21] *See, e.g.*, Fla. Stat. § 501.171.
[22] *See, e.g.*, Wash. Rev. Code § 19.255.010 *et seq.*
[23] *See e.g.*, Del. Code Ann. Tit. 6 § 12B-101 *et. seq.*
[24] *See, e.g.*, Conn. Gen. Stat. § 36a-701b.
[25] Fla. Stat. § 501.171.

provides that notification "must be made in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred . . . ."[26]

157. Based on the disclosure letters and online reports, LabCorp violated state statutes relating to timely notification by exceeding the statutory notice period of forty-five (45) days in Washington, which provides that notification "must be made in the most expedient time possible and without unreasonable delay, no more than forty-five calendar days after the breach was discovered . . . ."[27]

158. LabCorp violated the statutory notice period in Vermont, which provides that notification "shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification [of the breach.]"[28]

159. LabCorp also violated the statutory notice period in Oregon, which provides that notification "shall [be made] in the most expeditious manner possible, without unreasonable delay . . . but not later than 45 days after discovering or receiving notification of the breach of security."[29]

160. LabCorp additionally violated the statutory notice period in Alabama,

[26] Colo. Rev. Stat. § 6-1-716.
[27] Wash. Rev. Code § 19.255.010 *et seq.*
[28] 9 V.S.A. §§ 2430, 2435.
[29] Or. Rev. Stat. §§ 646A.600 – 646A.628.

which provides that notification "shall be made as expeditiously as possible and without unreasonable delay . . . the covered entity shall provide notice within 45 days . . . ."[30]

161. Based on the disclosure letters and online reports, LabCorp violated state statutes relating to timely notification by exceeding the statutory notice period of sixty (60) days in Louisiana, which provides that notification "shall be made in the most expedient time possible and without unreasonable delay but not later than sixty days from the discovery of the breach . . . ."[31]

162. The other states to which LabCorp provided notice of the First Breach have not established a bright-line threshold regarding notification after a data breach. Specifically, California requires that disclosure be made "in the most expedient time possible and without unreasonable delay[.]"[32] Additionally, California requires a breach of medical information to be disclosed "no later than 15 business days after the unlawful or unauthorized access, use, or disclosure has been detected[.]"[33] Maine requires disclosure to be made as "expediently as possible and without unreasonable delay[.]"[34] Indiana requires that disclosure shall be made "without

[30] Ala. Code § 8-38-1 *et. seq.*
[31] La. Rev. Stat. § 51:3071 *et seq.*
[32] Cal. Civ. Code § 1798.80 *et. seq.*
[33] Cal. Health & Safety Code § 1280.15.
[34] 10 Me. Rev. Stat. § 1346 *et. seq.*

unreasonable delay."[35] Montana requires that disclosure "must be made without unreasonable delay . . . ."[36] Nebraska requires that disclosure "shall be made as soon as possible and without unreasonable delay . . . ."[37] New Hampshire requires that notification shall be made "as soon as possible . . . ."[38] North Carolina requires that notification "shall be made without unreasonable delay . . . ."[39] Puerto Rico requires notification to be provided "as expeditiously as possible . . ." and regulators must be notified "[w]ithin a non-extendable term of ten (10) days after the violation of the system's security has been detected . . . ."[40] South Carolina requires that notification "must be made in the most expedient time possible and without unreasonable delay . . . ."[41] Illinois requires that notification "shall be made in the most expedient time possible and without unreasonable delay . . . ."[42] Massachusetts requires that notification shall be provided "as soon as practicable and without unreasonable delay . . . ."[43]

163. Although the states identified in ¶ 162 do not provide a hard deadline for notice, the states do require notice to be provided "without unreasonable delay"

[35] Ind. Code § 24-4.9-1-1 *et. seq.*
[36] Mont. Code §§ 30-14-1701-02,1704.
[37] Neb. Rev. Stat. § 87-801 *et. seq.*
[38] N.H. Rev. Stat. §§ 359-C:19-C:21; N.H. Rev. Stat. § 332-I:5.
[39] N.C. Gen. Stat. §§ 75-61, 75-65.
[40] P.R. Laws Tit. 10 § 4051 *et seq*.
[41] S.C. Code Ann. § 39-1-90.
[42] 815 Ill. Comp. Stat. 530/5 *et. seq.*
[43] Mass. Gen. Laws 93H § 1 *et. seq.*

and in an expeditious manner. LabCorp's delay in notifying affected patients is unreasonable as the company was put on direct notice of the First Breach on May 14, 2019, and knew or had reason to know, were reckless in not knowing, or should have known no later than March 2019; however, LabCorp willfully delayed providing notice to affected patients for at least sixty (60) days. By deliberately withholding notice from affected patients, LabCorp subjected its patients to an enhanced state of vulnerability as patients were unaware that their PII or PHI may have been exposed. Further, the Individual Defendants breached their duty of due care by failing to ensure that the Company provided notice in an expedient manner. Moreover, the wholly inadequate contents of the eventual notice and failure to timely notify patients as required by law caused the Company to violate numerous state and federal laws, and exposed the Company to likely fines and penalties.

164. The Company is also subject to a Consumer Class Action. The Consumer Class Action contains allegations surrounding LabCorp's failure to provide notice relating to the First Breach and its failure to act with due care with regard to its "business associate," AMCA.

165. The Individual Defendants, as directors and/or officers of LabCorp, are responsible for the ongoing potential liability caused by their willful and/or reckless violations of state notification statutes.

The Individual Defendants Breached Their Duty to Properly Secure LabCorp's Patients' Personal Information

166. The Individual Defendants have and had a continuing contractual and common-law duty and obligation to keep confidential the PII and PHI their patients disclosed to LabCorp and to protect this PII and PHI from unauthorized disclosure. These agreements, duties, and obligations are based on: (1) HIPAA; (2) industry standards; (3) the agreements, promises and representations made to LabCorp patients and shareholders; and (4) Section 5(a) of the Federal Trade Commission Act ("FTC ACT"), 15 U.S.C. § 15. LabCorp patients provided their PII and PHI to the Company with the reasonable belief that LabCorp and its business associates would comply with its agreements and any legal requirements to keep that PII and PHI confidential and secure from unauthorized disclosure.

167. HIPAA requires that LabCorp provide every patient it treats with a privacy notice.

168. In this HIPAA-mandated privacy notice, LabCorp agrees that it will keep PHI of its patients confidential and protected from unauthorized disclosure. In its Notice of Privacy Practices, posted on the Company's website and effective May 9, 2016, LabCorp promises and agrees, in relevant part:

> 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.

(Emphasis added).

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

170. LabCorp promises patients that it will keep their PII and PHI confidential, assuring patients that their financial "information **may be accessed only by LabCorp agents and employees who maintain password and position-required access rights, and third-party vendors who support LabCorp's billing operations.**"[44] (Emphasis added).

[44] LabCorp, *Website Privacy Policy* (Oct. 2, 2019), https://www.labcorp.com/hipaa-privacy/web-privacy-policy.

171. LabCorp's data security agreements, obligations, and commitments are particularly important given the substantial increase in data breaches (particularly in the healthcare industry) during the period preceding the First Breach. LabCorp's failure to provide the data-security protections it committed to provide to its patients was particularly egregious in light of specific government warnings regarding the possibility of attempts to illegally access the data of companies like LabCorp. Such warnings alerted LabCorp to the risk of a data breach and further emphasized LabCorp's duty to keep patients' PII and PHI secure and to ensure that its business associates, such as AMCA, kept its patients' PII and PHI secure, as HIPAA mandates. Additionally, these warnings put the Individual Defendants on notice that adequate corporate governance and policies and procedures were required to securely operate a business that acquired, retained, and transferred highly sensitive PII and PHI of patients.

172. As alleged above, AMCA was a "business associate" of LabCorp with whom LabCorp shared PII and PHI of LabCorp's patients. Indeed, LabCorp was one of AMCA's two largest clients. As LabCorp's business associate, AMCA was required to maintain the privacy and security of LabCorp patients' PII and PHI. HIPAA mandates that a covered entity (i.e., LabCorp) may only disclose PHI to a "business associate" (i.e., AMCA) if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes

for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[45] The Individual Defendants failed to ensure that the Company's business associate, AMCA, safeguarded the PII and PHI of LabCorp's patients and that AMCA complied with HIPAA's privacy mandates. In fact, the Individual Defendants failed to enforce contractual provisions between LabCorp and AMCA that are designed to protect patient PII and PHI.

The Individual Defendants and LabCorp Violated HIPAA's Requirements to Safeguard Data

173. LabCorp and the Individual Defendants had and have a non-delegable duty to ensure that all information collected, stored, and transmitted by the Company was secure and that any associated entities with whom they shared member information maintained adequate and commercially reasonable data security practices to ensure the protection of patients' PII and PHI.

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

[45] *See* 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and (e).

Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

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

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

177. HIPAA requires that the Company implement appropriate safeguards for this information.

178. HIPAA further mandates that a covered entity such as LabCorp may disclose PHI to a "business associate," such as AMCA, only if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[46]

179. HIPAA requires that the Company provide notice of a breach of unsecured protected health information, which includes PHI that is not rendered

[46] *See* 45 C.F.R. 164.502(e), 164.504(e), 164.532(d) and (e).

unusable, unreadable, or indecipherable to unauthorized persons – i.e. non-encrypted data.

180. Despite these requirements, LabCorp and the Individual Defendants failed to comply with their duties under HIPAA and their own Notice of Privacy Practices in regard to the First Breach (and, as discussed below, similarly failed to comply regarding the Second Breach). Indeed, the Company failed to:

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

b. Adequately protect patients' PII and PHI;

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

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

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

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

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

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

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

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

181. LabCorp and the Individual Defendants failed to comply with their duties and obligations under HIPAA and their own Code, despite being aware of the risks associated with unauthorized access of their patients' PII and PHI.

The Individual Defendants and LabCorp Were on Notice That Highly Valuable PII and PHI of Their Patients Could Be Breached

182. LabCorp and the Individual Defendants knew or had reason to know, were reckless in not knowing, or should have known that they were collecting highly valuable data, for which LabCorp and the Individual Defendants knew, or had reason to know, were reckless in not knowing, or should have known that such data was becoming increasingly sought after with an upward trend in data breaches in recent years.[47] Accordingly, LabCorp and the Individual Defendants were on notice for the harms that could result if they failed to protect their patients' PII and PHI.

183. HHS' Office for Civil Rights currently lists 568 breaches affecting 500 or more individuals in the past 24 months.[48] LabCorp patients damaged by the First Breach are the second largest group, following the Quest patients.

---

[47] HIPAA Journal, *Healthcare Data Breach Statistics*, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited April 17, 2020) ("Our healthcare statistics clearly show there has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published.").

[48] U.S. Dep't of Health and Human Services, Office for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Apr. 17, 2020).

184. As early as 2014, the FBI alerted the healthcare industry that it was an increasingly preferred target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)" so that these companies can take the necessary precautions to thwart such attacks.[49]

185. At the end of 2018, the healthcare sector ranked second highest in the number of data breaches among measured sectors and had the highest rate of exposure for each breach.[50] With the First Breach, 2019 has seen the exposure of three times the number of records compromised in 2018.[51]

186. The First Breach (and subsequently the Second Breach discussed below) contained data highly sought by hackers including: PII which can be used for identity fraud, PHI, and financial account information. Providing a "business associate," such as AMCA, with highly sensitive PII and PHI also increases a patient's susceptibility to a data breach and leads to questions as to whether LabCorp providing AMCA this type of PII and PHI was truly necessary. Hackers are able to

[49] Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, Reuters, Aug. 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.
[50] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, https://www.idtheftcenter.org/2018-data-breaches (last visited Apr. 17, 2019).
[51] HIPAA Journal, *August 2019 Healthcare Data Breach Report* (Sept. 23, 2019), https://www.hipaajournal.com/august-2019-healthcare-data-breach-report.

obtain multiple forms of information relating to a single individual and sell this information for a higher premium on the dark web. As such, limiting the amount of information provided to a "business associate," such as AMCA, would reduce the potential value of hacked data and, in turn, likely reduce the overall potential risk of hackers targeting companies like AMCA.

187. PII and PHI are a valuable commodity to identity thieves. Compromised PII and PHI 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 PII/PHI directly on various dark web sites making the information publicly available.[52]

188. Further, medical databases are particularly high value targets for identity thieves. According to one report, a stolen medical identity, such as PHI, has a $50 street value on the black market, whereas a Social Security number sells for only $1.[53]

[52] Brian Stack, Experian, *Here's How Much Your Personal Information Is Selling for on the Dark Web* (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/; 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 Apr. 17, 2019).

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

189. LabCorp and the Individual Defendants are or should be well aware that their own data and the data they share with AMCA contained a treasure trove of material for hackers, as the Company 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.

190. In a note to employees about the July 2018 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."

191. As stated in the Company's 2020 Proxy Statement, the Audit Committee comprised of Defendants Anderson, Davis, Gilliland, Neupert, and Williams "receives reports at its regularly scheduled meetings from the Chief Information Security Officer and the Chief Information Officer [Defendant Berberian]" relating to cybersecurity. As such, the members of the Audit Committee and Defendant Berberian knew or should have known of the cyber risks and threats facing the Company.

192. As stated in the Company's 2020 Proxy Statement, "the full Board receives briefings from the Chief Information Security Officer and the Chief

Information Officer [Defendant Berberian] twice per year." As such, all of the Director Defendants knew or should have known of the cyber risks and threats facing the Company.

193. Additionally, the Company is also subject to a Consumer Class Action. The Consumer Class Action contains allegations surrounding LabCorp's failure to provide notice relating to the First Breach, the Company's failure to protect and secure patient PII/PHI and violations of HIPPA.

LabCorp Suffers Second Data Breach

194. On January 28, 2020, *TechCrunch* published an article (the "*TechCrunch* Article") announcing that LabCorp suffered a Second Breach that exposed thousands of medical documents.[54] According to the *TechCrunch* Article, "[a] security flaw in LabCorp's website exposed thousands of medical documents, like test results containing sensitive health data."

195. The *TechCrunch* Article explains that "[a]lthough the system appeared to be protected with a password, the part of the website designed to pull patient files from the back-end system was left exposed. That unprotected web address was visible to search engines and was later cached by Google, making it accessible to anyone who knew where to look."

[54] Zack Whittaker, TechCrunch, *LabCorp security lapse exposed thousands of medical documents* (Jan. 28, 2020), https://techcrunch.com/2020/01/28/labcorp-website-bug-medical-data-exposed/.

196. The Second Breach allowed access to LabCorp documentation containing patients' health information. According to the *TechCrunch* Article, "at least 10,000 documents were exposed." Further, "[t]he documents contained names, dates of birth and, in some cases, Social Security numbers of patients. The documents also contained lab test results and diagnostic data, a class of data considered protected health information under the Health Insurance Portability and Accountability Act (HIPAA)." Additionally, certain documents contained a footnote that read: "[t]his document contains private and confidential health information protected under state and federal law."

197. According to Rachel Tobac, founder of SocialProof Security, which coins itself as "white hat hackers" who work to strengthen companies' first lines of defense, "[the Second Breach] is a massive privacy issue — and one that could impact affected users and patients for years to come . . . . The sensitive nature of those documents and the leak of private medical status is a huge privacy violation for those patients for obvious reasons, but also sadly for some possibly less glaring reasons, as well."[55] Tobac noted that medical information can be "terribly useful" for criminals in identity theft, extortion and phishing, because the victim may be more likely to trust the sender "under the assumption that the message is legitimate because it contains information only their medical provider could or should know."

[55] *Id.*

198. According to *TechCrunch*, LabCorp spokesman Donald Von Hogan stated, "I can confirm that we have terminated access to the system." Additionally, *TechCrunch*, "reached out to a number of patients to verify their information. Only one person confirmed by phone that the information in their exposed file was accurate[.]"

199. LabCorp and the Individual Defendants were well aware of their HIPPA obligations. In *Lee-Thomas v. LabCorp, Laboratory Corp. of America*, Docket No. 1:18-cv-00591-RC (D.D.C. Mar. 16, 2018), LabCorp faced a lawsuit premised on purported HIPPA violations surrounding the protection of PII and PHI that was not properly protected. Lee-Thomas alleged that the Company set-up computers for intake of PII and PHI in full view of any member of the public within a hospital.

LabCorp Failed to Disclose or Provide Proper Notice of the Second Breach

200. Although LabCorp was aware of the Second Breach reported by *TechCrunch* in January 2020, the Company has failed to disclose this breach in any widely disseminated public release or SEC filing. Shockingly, LabCorp's only acknowledgment of the Second Breach, beyond saying that the Company "terminated access to the system[,]" is the statement released after the *TechCrunch* Article was published, stating that LabCorp would notify affected patients "as may be appropriate," but would not say if it would inform state and federal authorities

under data breach notification laws. The statement suggests that LabCorp does not plan on notifying the thousands of victims of the Second Breach. Instead, LabCorp and the Individual Defendants will independently decide which affected patients are worthy of notification, which LabCorp may determine is none.

201. Unlike the First Breach, the Second Breach occurred on LabCorp's systems, and therefore, the Company cannot attempt to skirt responsibility surrounding notification and remediation of the Second Breach. However, LabCorp's selective response regarding providing notice to victims "as may be appropriate" and the uncertainty regarding state and federal notification regarding the Second Breach suggests that the Company and the Individual Defendants plan to provide minimal notice of the Second Breach.

202. By failing to disclose and notify the affected patients, the Individual Defendants are once again opening LabCorp up to fines, penalties, and lawsuits. Additionally, and as noted by the Senators' letter regarding the First Breach, the consistent issues LabCorp has surrounding data security and the protection of PII and PHI leads to a conclusion that LabCorp is unable or unwilling to protect confidential PII and PHI, nor is the Company capable of securing its internal systems.

203. The Second Breach demonstrates a pervasive reality that the internal procedures and controls, whether they exist or not, are severely deficient for

application in the modern technological world. Further, any procedures and policies that LabCorp may have established in order to adequately respond to a data incident are likewise deficient and lacking.

204. LabCorp was wholly unaware of the existence of the Second Breach and failed to detect the vulnerability with its system. Had *TechCrunch* not informed LabCorp of the Second Breach, the Company's system would have continued to expose patients' PII and PHI, as well as cause further harm to LabCorp patients.

205. The Individual Defendants failed to exercise due care in protecting patients' PII and PHI by allowing patient information to be transmitted over the internet through an unprotected web address.

206. Despite acknowledging that the First Breach will cost LabCorp millions of dollars, LabCorp and the Individual Defendants have not disclosed the Second Breach in any SEC filing.

DAMAGES TO LABCORP CAUSED BY THE INDIVIDUAL DEFENDANTS

207. As a direct and proximate result of the Individual Defendants' misconduct, the Individual Defendants allowed for materially inadequate controls over the Company's policies and practices, failed to exercise due care in contracting with AMCA, failed to protect patient PII and PHI, willfully or recklessly permitted LabCorp to violate state and federal laws, and substantially damaged the Company's credibility, corporate image, and goodwill.

208. LabCorp has expended and will continue to expend significant sums of money. Additional expenditures and damages that the Company has incurred as a result of the Individual Defendants' breaches of their fiduciary duty include:

a. Costs incurred from compensation and benefits paid to the Individual Defendants who have breached their duties to LabCorp;

b. Costs incurred to notify affected patients, state attorneys general, and federal and state agencies;

c. Costs incurred in the form of fines and penalties levied against the company with regards to violations of state and federal laws and regulations;

d. Costs related to the Company's loss of market credibility stemming from the inadequate disclosures and repeated data breaches; and

e. Costs incurred regarding the litigation brought against the company relating to the Data Breaches, including the Consumer Class Action.

209. In fact, LabCorp filed a Form 8-K with the SEC on February 13, 2020 indicating that for the twelve months ended December 31, 2019 the Company expended or plans to expend $11,500,000 in "[c]osts related to the response and remediation of a previously announced vendor data breach, which occurred in the second quarter of 2019." The Company has not yet disclosed any costs associated with the Second Breach.

210. Finally, LabCorp's credibility, reputation, and goodwill have likewise been damaged, and the Company remains exposed to significant potential liability going forward.

DERIVATIVE AND DEMAND FUTILITY ALLEGATIONS

211. Plaintiff brings this action derivatively in the right and for the benefit of LabCorp to redress injuries suffered, and to be suffered, by LabCorp as a direct result of the Individual Defendants' multiple breaches of fiduciary duty.

212. Plaintiff is a shareholder of LabCorp, was a shareholder of LabCorp at the time of the wrongdoing alleged herein and has been a shareholder of LabCorp continuously since that time.

213. Plaintiff will adequately and fairly represent the interests of the Company and its shareholders in enforcing and prosecuting its rights.

214. LabCorp is named as a nominal defendant in this case solely in a derivative capacity. This is not a collusive action to confer jurisdiction on this Court that it would not otherwise have. Prosecution of this action, independent of the current Board, is in the best interests of the Company.

215. The wrongful acts complained of herein subject, and will continue to subject, LabCorp to continuing harm because the adverse consequences of the actions are still in effect and ongoing.

216. The wrongful acts complained of herein were unlawfully concealed from LabCorp shareholders.

217. At the time this action was initiated, the Board was comprised of ten directors: Defendants King (Chairman), Anderson, Bélingard, Davis, Gilliland, Kong, Neupert, Parham, Schechter, and Williams.

218. [redacted]

219. [redacted]

220. [redacted]

[redacted]. As noted throughout this Complaint, LabCorp delayed notice to affected customers until July 13, 2019.

221. [redacted]

222. Even in the face of AMCA's bankruptcy, which was initiated on June 17, 2019, the Director Defendants continued to delay notice of the First Breach to LabCorp patients for nearly an additional month. Further, the Director Defendants wholly relied upon a bankrupt AMCA to establish and maintain identity protection and credit monitoring services for affected LabCorp patients. These conscious actions and inactions by the Director Defendants were in bad faith and violated the Director Defendants' duty of loyalty to the Company.

223. As a result of the facts set forth herein, Plaintiff has not made any demand on the Director Defendants to institute this action since a demand would be

a futile and useless act because a majority of the Director Defendants are incapable of making an independent and disinterested decision to institute and vigorously prosecute this action. The wrongful acts complained of herein show multiple breaches of their fiduciary duties of loyalty, care, and good faith.

224. All of the Director Defendants are disqualified from fairly evaluating the derivative claims because they are responsible for damages suffered by LabCorp as a result of the Data Breaches and the failure to timely notify the Company's patients. The Director Defendants are also responsible for delaying shareholder notification of the First Breach and failing to issue any public disclosure either in an SEC filing or other widely disseminated public announcement regarding the Second Breach. The Director Defendants' conscious inaction in the face of a duty to act constitutes bad faith and a breach of their duty of loyalty.

225. The Director Defendants' failure of oversight reflects a conscious and deliberate disregard of their fiduciary duties – namely, inaction in the face of circumstances that plainly called for immediate action. This constitutes bad faith. As such, the Director Defendants face a substantial likelihood of liability, rendering demand upon them futile. Further, the Director Defendants' conscious inaction evidences their inability and unwillingness to consider a demand to commence and vigorously prosecute this action.

226. The Director Defendants either issued or permitted the Company to issue materially false and misleading statements about the effectiveness of LabCorp's internal controls and procedures and the existence of the Data Breaches. The Director Defendants have made repeated conscious decisions not to adequately respond to the First Breach and to ignore the Second Breach. The Director Defendants also violated the Company's Code and the Company's Corporate Governance principles, including failing to ensure that systematic risks are being addressed and maintaining the integrity of the company with regard to its financial statements and other public disclosures, and compliance with law and ethics. The actions, or inaction, of the Director Defendants evidence their inability to consider a demand to commence and vigorously prosecute this action.

227. Further, the Director Defendants' intentional and knowing failure to disclose the Second Breach and concerted effort to shift the entirety of the responsibility of the First Breach to a bankrupt AMCA demonstrates that a demand upon the Director Defendants would be a futile and useless act.

228. There is also reasonable doubt that the Director Defendants' decisions were the product of a valid exercise of business judgment. The Director Defendants made multiple decisions following each of the Data Breaches whereby proper disclosure and prompt notification was consciously withheld from the affected individuals, proper governmental authorities, and the investing public.

229. After the First Breach, the Director Defendants were satisfied with a bankrupt AMCA notifying less than 2% of affected LabCorp patients, a mere 200,000 out of nearly 10.2 million affected LabCorp patients, and the Director Defendants delayed taking any further action for nearly sixty (60) days.

230. The Director Defendants indicated that after the Second Breach, affected patients would be notified "as may be appropriate," suggesting that the Director Defendants willingly withheld notification to affected patients.

231. Intentionally delaying and limiting notice to affected patients is not a valid exercise of business judgment. As such, demand would be futile.

232. According to the 2020 Proxy Statement, the Audit Committee convened meetings at least 8 times throughout 2019, or roughly twice per quarter. During these meetings the Audit Committee, consisting of Defendants Anderson, Davis, Gilliland, Neupert, and Williams (the "Audit Committee Defendants"), received reports and met with the Chief Information Security Officer and CIO to review cybersecurity issues, as well as respond to data breaches. The regular and consistent meetings of the Audit Committee indicate that the Audit Committee Defendants, constituting half of the Director Defendants, knew, should have known, were reckless in not knowing, or intentionally ignored, dismissed, or otherwise willfully disregarded both the First Breach and the Second Breach. The Audit Committee Defendants' failure to act upon a known duty to act in relation to the

Data Breaches is not a valid exercise of business judgment and constitutes bad faith. As such, demand upon the members of the Audit Committee would be futile.

233. Demand upon the Audit Committee Defendants would be futile. The Audit Committee Defendants failed to adequately perform their duties in accordance with the Company's Audit Committee Charter. Following the Data Breaches, the Audit Committee Defendants failed to respond to the Data Breaches, and further failed to inform, instruct, and/or otherwise report to the remaining Director Defendants. As a result, the Audit Committee Defendants face a substantial likelihood of liability for their breach of fiduciary duties.

234. Demand upon the members of the Quality and Compliance Committee, Defendants Bélingard, Davis, Gilliland, and Williams (the "Quality and Compliance Committee Defendants") would be futile. The Quality and Compliance Committee Defendants failed to adequately perform their duties in accordance with the Company's Quality and Compliance Committee Charter. Following the Data Breaches, the Quality and Compliance Committee Defendants failed to oversee the Company's compliance with legal and regulatory standards, including regulatory health laws. As a result, the Quality and Compliance Committee Defendants face a substantial likelihood of liability for their breach of fiduciary duties.

235. As aforementioned, the Audit Committee Defendants had and have a duty to monitor and maintain cybersecurity policies and procedures, respond to data

breaches, and inform all the Director Defendants as necessary. Additionally, the Quality and Compliance Committee Defendants have a duty to oversee the Company's legal and regulatory compliance, inclusive of state and federal health laws, and inform all the Director Defendants as necessary. Therefore, the Director Defendants knew, should have known, or were reckless in not knowing that the Company was in violation of state and federal laws relating to disclosure and notification following the Data Breaches, discussed above, which is not a valid exercise of business judgment. Accordingly, each Director Defendant faces a substantial likelihood of liability. As such, demand upon the Director Defendants would be futile.

236. The Director Defendants each knew the magnitude of damage that a data breach could cause, and that robust corporate governance and risk management procedures were required and necessary to protect LabCorp from being victimized. Nonetheless, the Director Defendants failed to properly protect the Company.

237. The Director Defendants refused to act in the face of numerous red flags demonstrating the insufficient data security practices of its vendor, AMCA, and the internal Company practices, and failed to implement controls designed to protect against a data breach. Moreover, the Director Defendants failed to adequately review and affirm or revise existing policies and procedures relating to data security,

even though third parties, including United States Senators, pointed out the issues surrounding the Company's data security.

238. The conscious and willful disregard of the importance and necessity of adequate internal controls and procedures to both protect patient PII/PHI and the Company from direct exposures, demonstrates the Director Defendants' unwillingness to act in the best interests of LabCorp. As such, the Director Defendants face a substantial likelihood of liability, and demand upon the Director Defendants would be futile.

239. The Director Defendants failed to properly respond once they became aware of the Data Breaches by not providing immediate notice to the impacted patients and not immediately disclosing the Data Breaches. Because of their failures to act in the face of a known duty to act to protect the Company, the Director Defendants face a substantial likelihood of liability, and demand against them would be futile.

240. As a result of the Director Defendants' failure to adequately respond to the First Breach and their failure to institute adequate controls, procedures, and policies, LabCorp is subject to a Consumer Class Action. The Consumer Class Action is premised on allegations and failures directly attributable to the action and/or inaction of the Director Defendants. As such, demand upon the Director Defendants would be futile.

241. LabCorp has been and will continue to be exposed to significant losses due to the wrongdoing complained of herein, yet the Director Defendants have not filed any lawsuits against themselves or others who were responsible for that wrongful conduct to attempt to recover for the Company any part of the damages LabCorp suffered and will continue to suffer.

242. Furthermore, demand on the Board would also be futile and is excused because the Director Defendants' decisions not to implement adequate corporate governance and risk management procedures necessary to protect the Company from a data breach serves no legitimate business purpose.

243. Based on the foregoing, the Director Defendants face a sufficiently substantial likelihood of liability and, accordingly, there is a reasonable doubt as to each Director Defendants' disinterestedness in deciding whether pursuing legal action would be in the Company's best interest. Additionally, the Director Defendants have repeatedly failed to act and have shown their unwillingness to disclose the Data Breaches, which indicates that demand upon the Director Defendants is futile. Accordingly, demand upon the Director Defendants is excused as being futile.

CAUSES OF ACTION

COUNT I

(Against the Director Defendants for Breach of Fiduciary Duty)

244. Plaintiff incorporates by reference and realleges each of the foregoing paragraphs as though fully set forth herein.

245. The Director Defendants owed and owe LabCorp fiduciary obligations, including the obligations of loyalty, good faith, and care. Among other things, the Director Defendants owed a fiduciary duty to LabCorp to disseminate truthful, accurate, and complete information to shareholders.

246. The Director Defendants breached their duties of loyalty, care, and good faith by: (i) failing to implement and enforce a system of effective internal controls and procedures to protect patients' PII and PHI; (ii) failing to exercise their oversight duties by not monitoring the Company's compliance with its own procedures and federal and state regulations; (iii) providing PII and PHI of patients to a business associate with deficient cybersecurity and breach detection; (iv) failing to ensure that the Company, as well as its business associates, utilized proper cybersecurity safeguards to adequately secure the PII and PHI; (v) failing to have a sufficient incident response plan to immediately respond to the Data Breaches; (vi) consciously disregarding, delaying, and failing to ensure that the Company notified all potentially affected individuals and entities in a timely manner upon discovering

the Data Breaches; (vii) failing to make adequate public disclosure of the Data Breaches; and (viii) allowing the Company to violate state and federal laws and regulations.

247. The Director Defendants had actual or constructive knowledge that the Company issued materially false and misleading statements, and they failed to correct the Company's public statements and representations. The Director Defendants had actual knowledge of the misrepresentations and omissions of material facts set forth herein, or acted with reckless disregard for the truth, in that they failed to ascertain and to disclose such facts even though such facts were available to them. Such material misrepresentations and omissions were committed knowingly, recklessly, with gross negligence, and/or in bad faith.

248. The Director Defendants had actual or constructive knowledge that the Company was engaging in the practices as set forth herein, and that internal controls were not adequately maintained.

249. As a direct and proximate result of the breaches of fiduciary obligations by the Director Defendants, LabCorp has sustained and continues to sustain significant damages, as alleged herein. As a result of the misconduct alleged herein, the Director Defendants are liable to the Company.

250. The Director Defendants' misconduct – through both their intentional actions and conscious inaction – cannot be exculpated under Delaware or other

applicable law as it implicated bad faith and a breach of the duty of loyalty.

251. Plaintiff, on behalf of LabCorp, has no adequate remedy at law.

COUNT II

(Against Defendant Schechter for Breach of Fiduciary Duty)

252. Plaintiff incorporates by reference and realleges each of the foregoing paragraphs as though fully set forth herein.

253. As the Company's CEO, Defendant Schechter owed and owes LabCorp fiduciary obligations, including the obligations of loyalty, good faith, and care. Among other things Schechter owed a fiduciary duty to LabCorp to disseminate truthful, accurate, and complete information to shareholders.

254. Schechter breached his duties of loyalty, care, and good faith by: (i) failing to implement and enforce a system of effective internal controls and procedures to protect patients' PII and PHI; (ii) failing to exercise their oversight duties by not monitoring the Company's compliance with its own procedures and federal and state regulations; (iii) providing PII and PHI of patients to a business associate with deficient cybersecurity and breach detection; (iv) failing to ensure that the Company, as well as its business associates, utilized proper cybersecurity safeguards to adequately secure the PII and PHI; (v) failing to have a sufficient incident response plan to immediately respond to the Data Breaches; (vi) consciously disregarding, delaying, and failing to ensure that the Company notified

all potentially affected individuals and entities in a timely manner upon discovering the Data Breaches; (vii) failing to make adequate public disclosure of the Data Breaches; and (viii) allowing the Company to violate state and federal laws and regulations.

255. Defendant Schechter had actual or constructive knowledge that the Company issued materially false and misleading statements, and he failed to correct the Company's public statements and representations. Schechter had actual knowledge of the misrepresentations and omissions of material facts set forth herein, or acted with reckless disregard for the truth, in that he failed to ascertain and to disclose such facts even though such facts were available to him. Such material misrepresentations and omissions were committed knowingly or recklessly.

256. Defendant Schechter had actual or constructive knowledge that the Company was engaging in the practices as set forth herein, and that internal controls were not adequately maintained.

257. As a direct and proximate result of the breaches of fiduciary obligations by Schechter, LabCorp has sustained and continues to sustain significant damages, as alleged herein. As a result of the misconduct alleged herein, Schechter is liable to the Company.

258. Defendant Schechter's misconduct – through both his intentional actions and conscious inaction – cannot be exculpated under Delaware or other

applicable law as it implicated bad faith and a breach of the duty of loyalty. Additionally, Schechter was acting in his capacity as an officer which cannot be exculpated under Delaware law.

259. Plaintiff, on behalf of LabCorp, has no adequate remedy at law.

COUNT III

(Against Defendants Berberian and Eisenberg ("the Officer Defendants") for Breach of Fiduciary Duty)

260. Plaintiff incorporates by reference and realleges each of the foregoing paragraphs as though fully set forth herein.

261. The Officer Defendants owed and owe LabCorp fiduciary obligations, including the obligations of loyalty, good faith, and care. Among other things, The Officer Defendants owed a fiduciary duty to LabCorp to disseminate truthful, accurate, and complete information to shareholders.

262. The Officer Defendants breached their duties of loyalty, care, and good faith by: (i) failing to implement and enforce a system of effective internal controls and procedures to protect patients' PII and PHI; (ii) failing to exercise their oversight duties by not monitoring the Company's compliance with its own procedures and federal and state regulations; (iii) providing PII and PHI of patients to a business associate with deficient cybersecurity and breach detection; (iv) failing to ensure that the Company, as well as its business associates, utilized proper cybersecurity safeguards to adequately secure the PII and PHI; (v) failing to have a sufficient

incident response plan to immediately respond to the Data Breaches; (vi) consciously disregarding, delaying, and failing to ensure that the Company notified all potentially affected individuals and entities in a timely manner upon discovering the Data Breaches; (vii) failing to make adequate public disclosure of the Data Breaches; and (viii) allowing the Company to violate state and federal laws and regulations.

263. The Officer Defendants had actual or constructive knowledge that the company issued materially false and misleading statements, and they failed to correct the Company's public statements and representations. The Officer Defendants had actual knowledge of the misrepresentations and omissions of material facts set forth herein, or acted with reckless disregard for the truth, in that they failed to ascertain and to disclose such facts even though such facts were available to them. Such material misrepresentations and omissions were committed knowingly or recklessly.

264. The Officer Defendants had actual or constructive knowledge that the Company was engaging in the practices as set forth herein, and that internal controls were not adequately maintained.

265. As a direct and proximate result of the breaches of fiduciary obligations by the Officer Defendants, LabCorp has sustained and continues to sustain significant damages, as alleged herein. As a result of the misconduct alleged herein,

the Officer Defendants are liable to the Company.

266. The Officer Defendants' misconduct – through both their actions and conscious inaction – cannot be exculpated under Delaware or other applicable law as it implicated bad faith and a breach of the duty of loyalty. Additionally, the Officer Defendants were acting in their capacity as officers which cannot be exculpated under Delaware law.

267. Plaintiff, on behalf of LabCorp, has no adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment as follows:

A. Determining that this action is a proper derivative action maintainable under the law and demand was excused;

B. Directing the Individual Defendants to account to LabCorp for all damages sustained or to be sustained by the Company by reason of the wrongs alleged herein;

C. Directing LabCorp to take all necessary actions to reform its corporate governance and internal procedures to comply with applicable laws and protect the Company and its shareholders from a recurrence of the events described herein, including, but not limited to, a shareholder vote for amendments to LabCorp's By-Laws or Articles of Incorporation, appointing or creating a Board-level committee and executive officer position specifically tasked with the oversight of data security,

and taking such other action as may be necessary to place before shareholders for a vote on corporate governance policies;

D. Ordering that the Individual Defendants issue a widely disseminated disclosure concerning the Second Breach in either, or both, an SEC filing or other widely disseminated public announcement;

E. Awarding to LabCorp restitution from the Individual Defendants and ordering disgorgement of all profits, benefits and other compensation obtained by the Individual Defendants;

F. Awarding to Plaintiff the costs and disbursements of this action, including reasonable attorneys' and experts' fees and expenses; and

G. Granting such other and further relief as the Court may deem just and proper.

[signature block on following page]

Dated: April 23, 2020

Respectfully submitted,

FARUQI & FARUQI, LLP

/s/ Michael Van Gorder
Michael Van Gorder
Del. Bar ID No. 6214
3828 Kennett Pike
Suite 201
Wilmington, Delaware 19807
Telephone: 302-482-2500
Facsimile: 302-482-3612
mvangorder@faruqilaw.com

OF COUNSEL:

FARUQI & FARUQI, LLP

Alex B. Heller
Christopher M. Lash
1617 John F. Kennedy Blvd, #1550
One Penn Center
Philadelphia, PA 19103
Telephone: 215-277-5770
Facsimile: 215-277-5771
aheller@faruqilaw.com
clash@faruqilaw.com

Attorneys for Plaintiff Raymond Eugenio