Exhibit A

James E. Cecchi
CARELLA BYRNE CECCHI
OLSTEIN BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
(973) 994-1700
Interim Lead Counsel for Plaintiffs
(Additional Counsel on the Signature Page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE: AMERICAN MEDICAL COLLECTION AGENCY, INC. CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: Other Labs Track	Civil Action No. 19-md-2904 (MCA)(MAH) **FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT: SONIC HEALTHCARE USA AND RELATED SUBSIDIARIES AND LABORATORIES**

TABLE OF CONTENTS

TABLE OF CONTENTS
(Cont'd)

Page

Plaintiffs, individually and on behalf of classes of all those similarly situated (the "Class" or "Class Members"), upon personal knowledge of the facts pertaining to Plaintiffs and on information and belief as to all other matters, and upon the investigation conducted by Plaintiffs' counsel, bring this class action complaint against Sonic Healthcare USA ("Sonic"), and its subsidiaries, Clinical Pathology Laboratories, Inc. ("CPL") and Aurora Diagnostics LLC ("Aurora") as well as Aurora's subsidiary, Austin Pathology Associates (collectively, "Defendants")[1] and allege as follows:

PRELIMINARY STATEMENT

1. In July 2019, several of Sonic and Aurora's subsidiaries—including named Defendants in this case—began to inform patients to whom they provided various healthcare services that an unauthorized user or users accessed the system run by their standardized billing collections vendor, Retrieval-Masters Creditor's Bureau, Inc., d/b/a American Medical Collection Agency ("AMCA"), between August 2018 and March 2019 (the "Data Breach"). After accessing AMCA's unprotected systems, the malicious actors exfiltrated the sensitive personal, financial, and medical information (including physician names, tests ordered, and diagnosis codes that represent conditions and diseases) of millions of Defendants' patients, which was subsequently made available on the illegal marketplace known as the "dark web."

2. Plaintiffs and Class Members entrusted Defendants with, and allowed Defendants to gather, highly sensitive information relating to their health and other matters as part of seeking treatment. They did so in confidence, and they had the legitimate expectation that Defendants would respect their privacy and act appropriately, including only sharing their information with

[1] As additional facts come to light, Plaintiffs may respectfully seek leave to amend this Complaint in order to bring additional causes of action by plaintiffs from other states.

vendors and business associates who legitimately needed the information and were equipped to protect it.

3. Defendants have a duty to secure and safeguard patient information entrusted to them. Defendants could have prevented this theft had they limited the patient information they shared with their vendors and business associates and employed reasonable measures to assure their vendors and business associates implemented and maintained adequate data security measures and protocols to secure and protect Defendants' patients' data.

4. Plaintiffs bring this class action because Defendants collected and failed to secure and safeguard their patients' protected health information ("PHI") and personally identifiable information ("PII")—such as Plaintiffs' and Class Members' names, mailing addresses, phone numbers, dates of birth, Social Security numbers, genders, information related to Plaintiffs' and Class Members' medical providers and services (such as dates of service, diagnosis codes, tests ordered, patient identification numbers, and referring doctor) and other private information—such as credit and debit card numbers, bank account information, insurance, insurance subscriber identification number (all collectively referred to as "Personal Information").

5. As of today, millions of Defendants' patients have had their Personal Information compromised as a result of the Data Breach. As a result of Defendants' failure to protect the Personal Information that Plaintiffs and Class Members were entrusted—and legally obligated—to safeguard, Plaintiffs and Class Members suffered a loss of value of their Personal Information and have been exposed to and/or are at imminent and significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. In fact, numerous Class Members are already victims of fraud.

6. Defendants could have prevented this theft had they limited the Personal Information of their patients that they shared with business associates and employed reasonable measures to assure their business associates implemented and maintained adequate data security measures and protocols to secure and protect their patients' Personal Information.

7. Defendants' intentional, willful, reckless, unfair, and/or negligent conduct—failing to prevent the Data Breach, failing to limit its severity, failing to detect it in a timely fashion, and failing to timely notify Plaintiffs and the Class—harmed Plaintiffs uniformly. As discussed herein, fraudulent activities have already been linked to Defendants' unfair and deceptive conduct. For this reason, Defendants should pay for appropriate identity-theft protection services and reimburse Plaintiffs and the Class for the costs caused by Defendants' sub-standard security practices and failure to timely disclose the same. Plaintiffs and the Class are also entitled to injunctive and other equitable relief that safeguards their Personal Information, requires Defendants to significantly improve their security, and provides independent, expert oversight of Defendants' security systems.

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

JURISDICTION AND VENUE

9. This First Amended Consolidated Complaint is intended to serve as an administrative summary as to all other complaints consolidated in this multidistrict litigation asserting claims against Defendants and shall serve for all purposes as an administrative device to aid efficiency and economy for the Class defined below. As set forth herein, this Court has general jurisdiction over Defendants and original jurisdiction over Plaintiffs' claims.

10. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 putative Class Members, and minimal diversity exists as Defendants and at least one Class Member are citizens different states.

11. This Court has personal jurisdiction over Defendants because they maintain sufficient minimum contacts in New Jersey such that they intentionally avail themselves of this Court's jurisdiction by conducting operations here, have patients located here, and contracts with companies in this District. Additionally, the United States Panel on Multidistrict Litigation transferred all related matters to this District, so Plaintiffs are bringing their claims against Defendants in this litigation before this Court.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1407 and the July 31, 2019 Transfer Order of the Judicial Panel on Multidistrict Litigation in MDL 2904 or, in the alternative, pursuant to 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this District. Venue is additionally proper because Defendants transact business and may be found in this District.

NAMED PLAINTIFFS

13. Plaintiffs are individuals who, upon information and belief, had their Personal Information compromised in the Data Breach after having medical services performed at Sonic and Aurora subsidiaries, and bring this action on behalf of themselves and all those similarly situated both across the United States and within their State or Territory of residence. These allegations are made upon information and belief derived from, *inter alia*, counsel's investigation, public sources—including sworn statements, Defendants' websites, and the facts and circumstances currently known. Because Defendants have exclusive but incomplete knowledge of what information was compromised for each individual, including PHI, Plaintiffs reserve the right to supplement their allegations with additional facts and injuries as they are discovered.

14. Each and every Plaintiff has suffered a concrete and particularized injury as a result of Defendants' failure to protect their Personal Information and its subsequent disclosure to unauthorized parties without their consent.

15. Had Defendants disclosed that they disregarded their duty to safeguard and protect Plaintiffs' Personal Information from unauthorized access, Plaintiffs would have taken this into account in making their healthcare decisions. In particular, had Plaintiffs known about Defendants' failure to ensure their vendors and business associates reasonably or adequately secured, safeguarded, and otherwise protected Plaintiffs' Personal Information, they would not have provided their Personal Information to Defendants and would have engaged a competing provider.

16. Plaintiff Gwendolyn Anderson ("Anderson") is a citizen and resident of the state of Texas.

17. Plaintiff Anderson was a CPL and Austin Pathology Associates ("Austin Pathology") patient who went to CPL and Austin Pathology to obtain blood testing on several occasions from 2015 through 2019.

18. Plaintiff Anderson provided CPL and Austin Pathology with her Personal Information as part of obtaining blood testing.

19. Plaintiff Anderson's bills from CPL and Austin Pathology were subsequently sent by CPL, Austin Pathology, and their parent companies, Sonic and Aurora (or Aurora's billing vendors McKesson Company or Change Healthcare), to Defendants' billing-collections vendor, AMCA.

20. As part of billing-collections services provided for Defendants, Plaintiff Anderson has been contacted through several letters by AMCA, including regularly receiving bills between 2015 and 2019, and in response, Plaintiff Anderson provided Personal Information to AMCA.

21. On July 15, 2019, Plaintiff Anderson received a letter from CPL regarding the Data Breach at AMCA, stating that her Personal Information may have been compromised.

22. On July 24, 2019, Plaintiff Anderson received a letter from Austin Pathology regarding the Data Breach at AMCA, stating that her Personal Information may have been compromised.

23. As a CPL and Austin Pathology patient, Plaintiff Anderson believed that CPL and Austin Pathology would protect her Personal Information once she provided it to CPL and Austin Pathology or their parent companies, Sonic and Aurora, and vendors.

24. Plaintiff Anderson would not have provided Defendants with this Personal Information nor used CPL and Austin Pathology to provide blood testing, had she known that they would fail to protect her Personal Information.

25. Plaintiff Anderson suffered and will continue to suffer damages due to the Data Breach. For example, in 2017, Plaintiff Anderson was the victim of fraudulently being provoked to pay approximately $400 in connection with her son's student loans, which is money that she has never received back. In 2018, Plaintiff Anderson's Gmail, Yahoo! Email, and Facebook accounts were all hacked. The hacker has been messaging Plaintiff Anderson's contacts to make requests. As a result of these breaches, Plaintiff Anderson has decided to pay over $100 annually for a credit-monitoring service. Plaintiff Anderson's credit was adversely affected as a result of the Data Breach.

26. In April 2020, as a result of the Data Breach, Anderson experienced at least one fraudulent charge to a website called Vudu.com of approximately $15 (that she did not pay) on her credit card, which was the same card used for expenses from CPL and Austin Pathology (amongst other expenses, including being given to AMCA for CPL and Austin Pathology bills). As a result, she has been forced to close credit and debit cards and open new ones, and she constantly receives robocalls. Plaintiff Anderson's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

27. Plaintiff Anderson has spent substantial time devoted to mitigating the adverse consequences of this Data Breach. For example, to date, she has spent several hours on monitoring her credit and financial accounts for any unauthorized activity, a practice that she will need to continue indefinitely to protect against fraud and identify theft.

28. Plaintiff Daniel Davis ("Davis") is a citizen and resident of the state of Texas.

29. Plaintiff Davis was a patient who went to CPL to obtain blood testing on several occasions as early as 2015, including, without limitation, on or about March 19, 2015 and December 11, 2017.

30. Plaintiff Davis provided CPL with his Personal Information as part of obtaining blood testing.

31. Plaintiff Davis' bills from CPL were subsequently sent to its billing collection vendor, AMCA, by CPL and its parent company, Sonic.

32. As part of billing-collections services provided for Defendants, Plaintiff Davis has been contacted through several letters by AMCA, including, without limitation, as recently as August 20, 2018, and in response, Plaintiff Davis provided Personal Information to AMCA.

33. On July 15, 2019, Plaintiff Davis received a letter from CPL regarding the Data Breach at AMCA, stating that his Personal Information may have been compromised.

34. As a Sonic patient, Plaintiff Davis believed that Sonic and its subsidiary, CPL, would protect his Personal Information once he provided it to Sonic, its subsidiaries, or its vendors.

35. Plaintiff Davis would not have provided any of the Defendants with this Personal Information nor used CPL to provide blood testing had he known that they would fail to protect his Personal Information.

36. Plaintiff Davis suffered and will continue to suffer damages due to the Data Breach. For example, on or around April 6, 2018, Plaintiff Davis suffered fraud when he was notified by his bank that someone tried to fraudulently withdraw approximately $1,700 from his account. Plaintiff Davis was forced to take at least one day off of work to close his bank account, credit cards, and debit cards, and he then had to open a new bank account and get new cards. His credit score has been adversely affected as a result of the Data Breach. As a result of the Data Breach, he has spent over a few hundred dollars a year in total on paying for anti-virus for his home computer and mobile phone. Plaintiff Davis's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

37. Plaintiff Davis has spent substantial time to mitigate the adverse consequences of the Data Breach. For example, to date, he has spent about an hour per week to monitor his credit and financial accounts for any unauthorized activity. Plaintiff Davis will continue to suffer damages due to the Data Breach, including, expending additional time and effort investigating the Data Breach, monitoring his checking and savings accounts to detect fraudulent activity, and the threat of future, additional harm including, without limitation, credit-card theft, identify theft, false-tax-return information submitted, a false loan submitted, expenses for credit monitoring, expenses for lifting credit-security freezes, and reduced credit scores.

38. Plaintiff Tonda Tate ("Tate") is a citizen and resident of the state of Texas.

39. Plaintiff Tate was a patient who went to CPL to obtain blood testing as early as 2018 and during 2019, including, without limitation, on July 24, 2018, April 18, 2019, and May 22, 2019.

40. Plaintiff Tate provided CPL with her Personal Information as part of obtaining blood testing.

41. On information and belief, Plaintiff Tate's bills from CPL, were subsequently sent by Sonic and CPL to their billing collection vendor, AMCA.

42. As a Sonic and CPL patient, Plaintiff Tate believed that Sonic and CPL would protect her Personal Information once she provided it to Defendants or their vendors.

43. On July 15, 2019, Plaintiff Tate received a letter from CPL regarding the Data Breach at AMCA, stating that her Personal Information may have been compromised.

44. Plaintiff Tate would not have provided CPL or any of the Defendants with this Personal Information nor used CPL to provide blood testing, had she known that they would fail to protect her Personal Information.

45. Plaintiff Tate suffered and will continue to suffer damages due to the Data Breach. On March 19, 2020, a fraudulent account was added to her TransUnion credit report which she was advised could definitely impact her credit score. Plaintiff Tate's personal information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

46. Plaintiff Tate has also spent substantial time to mitigate the adverse consequences of this Data Breach. For example, to date, Plaintiff Tate has spent several hours (including one hour per week) monitoring her credit and financial accounts for any unauthorized activity, a practice that she will need to continue indefinitely to protect against fraud and identify theft. Plaintiff Tate suffered and will continue to suffer damages due to the Data Breach, including, expending additional time and effort investigating the Data Breach, monitoring her checking and savings accounts to detect fraudulent activity, and the threat of future, additional harm including, without limitation, credit-card theft, identify theft, false-tax-return information submitted, a false loan submitted, expenses for credit monitoring, expenses for lifting credit-security freezes, and reduced credit scores.

DEFENDANTS

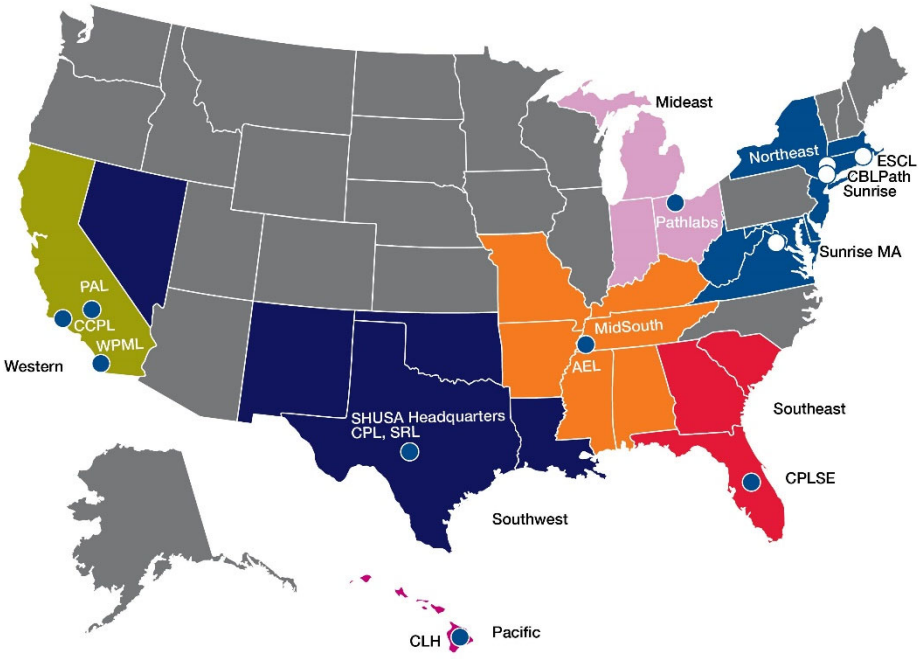
47. Defendant Sonic Healthcare USA, Inc. ("Sonic") is a corporation existing under the laws of the State of Delaware with its headquarters and principal place of business located in Austin, Texas. It is the parent company of Defendants Aurora and CPL, as well as its other laboratories: American Esoteric Laboratories, CBLPath, Inc., Sunrise Medical Laboratories, Inc.[2]

[2] *See, e.g., Our Divisions*, Sonic Healthcare USA, https://www.sonichealthcareusa.com/our-divisions/all-laboratories/ (last accessed Nov. 12, 2019); Bloomberg Law, Sonic Healthcare Ltd., Company Hierarchy, https://www.bloomberglaw.com/company/hierarchy/SHL%20AU%20Equity/results/022c46746635723c7d98cf895f741736 (last accessed Nov. 10, 2019); Sonic PROD 0001 (organization chart).

48. Sonic is also a "management company" of Defendant CPL, as well as its other subsidiaries American Esoteric Laboratories, CBLPath, and Sunrise Medical Laboratories. Sonic calls these labs "Sonic Divisions."

49. Sonic describes itself as "third largest laboratory medicine company in the United States, with operations across the country."

50. Sonic depicts its US operations as the following:



51. Defendant CPL is a subsidiary of Sonic and one of its laboratories. It is a corporation existing under the laws of the State of Texas with its headquarters and principal place of business located in Austin, Texas.

52. American Esoteric Laboratories ("AEL") is a subsidiary of Sonic and one of its laboratories. It is a corporation existing under the laws of the State of Delaware with its principal place of business in Memphis, Tennessee.

53. Sunrise Medical Laboratories ("Sunrise") is a subsidiary of Sonic and one of its laboratories. It is a corporation existing under the laws of the State of New York with its principal place of business in Hicksville, New York.

54. CBLPath, Inc. ("CBLPath") is a subsidiary of Sonic and one of its laboratories. It is a corporation existing under the laws of the State of Florida with its headquarters and principal place of business located in Rye Brook, New York.

55. Defendant Aurora Diagnostics, LLC ("Aurora") is a subsidiary of Sonic and one of its wholly-owned companies. It is a limited liability company existing under the laws of the State of Delaware, with its principal place of business in Palm Beach Gardens, Florida.[3] Aurora owns and is the management company of Defendant Austin Pathology Associates as well as its other subsidiaries: Laboratory Medicine Consultants, Ltd., South Texas Dermatology Lab, PLLC, Pathology Solutions, LLC, Seacoast Pathology, Inc., Arizona Dermatopathology, Western Pathology Consultants, Ltd., and Laboratory of Dermatology ADX, LLC (collectively "Aurora subsidiaries").

56. Aurora depicts its operations as follows[4]:

[3] Nine Aurora-affiliated labs were impacted by the Data Breach. *See* Marianne Kolbasuk McGee, *AMCA Breach Victim Count Continues to Grow*, info Risk Today (Aug. 14, 2019), https://www.inforisktoday.com/amca-breach-victim-count-continues-to-grow-a-12917.

[4] *See* Aurora Diagnostics, *Locations*, https://www.auroradx.com/locations/ (last accessed Mar. 29, 2022).

57. Defendant Austin Pathology Associates is owned and managed by Aurora and one of its pathology services. It is a medical group existing under the laws of the State of Texas with its principal place of business in Austin, Texas.

58. Laboratory Medicine Consultants, Ltd. ("LMC") is owned and managed by Aurora. It is a Nevada professional corporation with its principal place of business in Clark County, Nevada.

59. South Texas Dermatopathology Lab, PLLC, ("South Texas") is owned and managed by Aurora, and one of its dermatopathology practices. It is a Texas professional limited liability company with its principal place of business in San Antonio, Texas.

60. Pathology Solutions, LLC ("PS") is owned and managed by Aurora, and one of its pathology practices. It is a New Jersey limited liability company with its principal place of business in Eatontown, New Jersey.

61. Seacoast Pathology, Inc. ("Seacoast") is owned and managed by Aurora and one of its pathology services. It is a corporation existing under the laws of the State of New Hampshire with its principal place of business in Exeter, New Hampshire.

62. Arizona Dermatopathology ("AD") is owned and managed by Aurora and one of its full-service dermatopathology laboratories. It is a corporation existing under the laws of the State of Arizona with its principal place of business in Scottsdale, Arizona.

63. Western Pathology Consultants, Ltd. ("WPC") is owned and managed by Aurora and one of its providers of both inpatient and outpatient anatomic and clinical pathology services. It is a Nevada domestic professional corporation with its principal place of business in Reno, Nevada.

64. Laboratory of Dermatology ADX, LLC ("LDP") is owned and managed by Aurora and one of its dermatopathology services. It is a limited liability company existing under the laws of the State of New York with its principal place of business in Woodbury, New York.

FACTUAL ALLEGATIONS

I. Sonic Healthcare USA's rapid expansion and control over a variety of healthcare providers.

65. Sonic is a division of Sonic Healthcare Limited ("Sonic Limited"), one of the largest diagnostic laboratory medicine companies in the world and the third largest in the United States. According to Sonic's website, its members "focus on delivering the highest quality laboratory information through our unique Medical Leadership model and federated structure,

through regional diagnostic laboratories operating across the United States."[5]

66. Sonic touts its "relationships with hospitals and health systems" which "include joint venture partnerships, laboratory service agreements, and test sharing agreements" to provide numerous benefits to hospitals and patients. Among those benefits are: "[i]mproved integration of inpatient and outreach laboratory testing services, including electronic health records (EHR) integration," and "[d]etailed laboratory and clinical data that can reduce downstream healthcare costs."[6]

67. Sonic Limited's expansion into the United States began in 2005 with the acquisition of Clinical Pathology Laboratories ("CPL") of Austin, Texas. Since that time, Sonic has purchased other operating clinical and anatomic pathology laboratories across the country. At present there are nine operating divisions within Sonic with more than 7,000 employees providing clinical and anatomic pathology services to 20 million physicians and patients in 26 states.[7]

68. Sonic's expansion after the acquisition of Defendant CPL also included American Esoteric Laboratories and Sunrise Medical Laboratories (both acquired in 2007), and CBLPath (acquired in 2010).[8]

69. In early 2019, Sonic closed its acquisition of Defendant Aurora, a provider of anatomical pathology services. Aurora owns and manages Defendant Austin Pathology

---

5 *Welcome to Sonic Healthcare USA*, Sonic Healthcare USA, https://www.sonichealthcareusa.com (last accessed Mar. 29, 2022).

6 *About Us*, Sonic Healthcare USA, https://www.sonichealthcareusa.com/about-us/hospital-lab-partnerships/ (last accessed Nov. 13, 2019).

7 *Id.*

8 *Who We Are, History Detail*, Sonic Healthcare USA, https://www.sonichealthcareusa.com/about-us/who-we-are/history-detail/ (last accessed Nov. 13, 2019).

Associates, as well as its other subsidiaries: Laboratory Medicine Consultants, Ltd., South Texas Dermatopathology Lab, PLLC, Pathology Solutions, LLC, Seacoast Pathology, Inc., Arizona Dermatopathology, Western Pathology Consultants, Ltd., and Laboratory of Dermatology ADX, LLC.[9]

70. Aurora describes itself as "a leading independent pathology services and cancer diagnostics company, offering integrated diagnostic and personalized medicine consultations and information technology solutions to physicians and hospital systems."

71. Aurora also touts its "client-centric approach to providing diagnostic services" that "is driven by [its] belief that the practice of medicine and the delivery of healthcare are both personal and best delivered locally."

A. Sonic and Aurora acknowledge and commit to follow applicable privacy and security standards.

72. Sonic's Foundation Principles provide "clear guidelines about the interaction between Sonic's people and its external customers—primarily patients, doctors[,] and healthcare organisations. These principles form the foundations of our Medical Leadership culture and act as the operational drivers that ensure that each of our businesses remain focused on the needs of patients and their referring doctors."[10]

73. Additionally, Sonic's Values make the confidentiality of patient information paramount, and it promises "[t]o keep all information pertaining to patients, as well as professional

[9] Sonic Healthcare closes $540M acquisition of Aurora Diagnostics, S&P Global Marketplace (Jan. 31, 2019), https://www.spglobal.com/marketintelligence/en/news-insights/trending/FnpP2-Un2JlBZkt-r-GBqA2; *Locations*, Aurora Diagnostics, https://www.auroradx.com/locations/ (last accessed Nov. 13, 2019).

[10] *Foundation Principles*, Sonic Healthcare USA, https://www.sonichealthcareusa.com/sonic-healthcare/foundation-principles/ (last accessed Nov. 13, 2019).

and commercial issues, in strict confidence."[11] Its Values also include "tak[ing] ownership of each situation to the best of our ability, and to seek help when needed."[12] Sonic's representations continue:

> Our values were established in early 2000 after broad consultation with 5,000 employees across all of our practices. Their collective responses were distilled into a set of core values that act as a roadmap of how we want to behave as a company. These values apply to every single Sonic employee, regardless of their role or their country of operation.[13]

74. Sonic's Foundation Principles and Values are served by "external quality assurance certifications."[14] Sonic ensures that all of its laboratories and diagnostic centers "are fully accredited by the relevant regulatory bodies in the corresponding jurisdictions."[15] Sonic's quality assurance continues:

> This compliance is overseen by quality management teams that include medical, scientific, quality and administrative personnel within each business. These quality teams work objectively to ensure our medical facilities and supporting operations comply with the standards set down by relevant regulations and reflect good management and clinical practice at all times. The quality teams also perform an ongoing 'checks and balances' function that contributes to policy-making, planning, regular peer reviews and continuing professional development. To assist in the ongoing quality improvement process, a customised quality management software system, SmartLab, has been developed by Sonic, which enables collaboration and benchmarking for quality improvement across the laboratory medicine group. In FY2018, more than 750 formal quality accreditations and audits were performed by external quality agencies, and all Sonic facilities maintained their accreditation. A further 4,200 internal quality audits or reviews were carried out by qualified staff across the Sonic group, and all findings were resolved and fed

---

11 *Our Values*, Sonic Healthcare USA, https://www.sonichealthcareusa.com/sonic-healthcare/our-values/ (last accessed Nov. 13, 2019).

12 *Id.*

13 *Id.*

14 *Corporate Responsibility Report* at 19, Sonic Healthcare USA (2018), *available at* https://www.sonichealthcare.com/media/3915/shl_corporateresponsibilityreport_2018_web.pdf.

15 *Id.*

into the continuous improvement process.[16]

75. Despite its "federated" model allowing its labs to make decisions at the local level, Sonic exerts a great deal of control over its divisions, subsidiaries, agents, laboratories, facilities, employees, doctors, and suppliers. For example, Sonic directed its subsidiaries to cease using AMCA as a collection agency following the Data Breach. Sonic provides Information Technology ("IT") services for its subsidiaries. Sonic mandates its subsidiaries follow policies and procedures Sonic has created. Sonic provides patient billing services for its subsidiaries.

76. Sonic also requires all major suppliers, service providers, and any other agents or contracted third parties to adopt ethical and sustainable approaches to business that are consistent with Sonic's standards—including agreeing to comply with laws, regulations, and governmental requirements and directions.[17]

77. Aurora also acknowledges and commits to follow applicable privacy and security standards. Aurora has implemented privacy practices that are applicable to Aurora and all of its subsidiaries.

78. These privacy practices state Aurora and its subsidiaries are "committed" to the protection of patients' PHI and will make "reasonable efforts" to ensure the confidentiality of their patients' PHI.

79. Sonic and Aurora are also well aware of the Health Insurance Portability and Accountability Act's ("HIPAA") requirements regarding patient privacy and have both adopted a Notice of Privacy Practices for Protected Health Information ("PHI").

80. Sonic's Notice of Privacy acknowledges that it may supply PHI to "other

---

16 *Id.*

17 *Id.* at 20.

companies or individuals that needs the information to provide services to us. These other entities, known as 'business associates,' are required to maintain the privacy and security of PHI. For example, we may provide information to companies that assist us with billing of our services. We may also use an outside collection agency to obtain payment when necessary."[18]

81. Similarly, Aurora's Notice of Privacy acknowledges Aurora and its subsidiaries "may disclose PHI to persons or entities known as 'Business Associates' to perform specific functions or provide certain services to Aurora, to include other companies that provide billing services to Aurora's labs. All of Aurora's Business Associates are required to safeguard the privacy of your PHI."[19]

82. Sonic and Aurora also acknowledge in their respective privacy policies that they are required to notify patients in the event of a breach of unsecured PHI.[20]

B. Sonic, Aurora, and their respective subsidiaries contract with AMCA to provide billing collection services.

83. Defendants Sonic, Aurora, and their subsidiaries offer a variety of healthcare services to patients across the country.

84. Defendant CPL, a subsidiary of Sonic, offers laboratory services to patients at over

---

[18] Notice of Privacy Practices for Protected Health Information, Sonic Healthcare USA, https://www.sonichealthcareusa.com/home/privacy/ (last accessed Nov. 13, 2019).

[19] *See* Aurora Diagnostics' Notice of Privacy Practices, www.auroradx.com%2Fadxwp%2Fdownloads%2FHIPAA_Notice_of_Privacy_Practices.pdf (last accessed Mar. 29, 2022).

[20] Notice of Privacy Practices for Protected Health Information, Sonic Healthcare USA, https://www.sonichealthcareusa.com/home/privacy/ (last accessed Nov. 13, 2019); Aurora Diagnostics' Notice of Privacy Practices, www.auroradx.com%2Fadxwp%2Fdownloads%2FHIPAA_Notice_of_Privacy_Practices.pdf (last accessed Mar. 29, 2022)..

200 locations in eight states.[21] Patients visit CPL for laboratory testing following an order from a healthcare provider. CPL offers a range of pathology services including, biochemistry, microbiology, genetics, hematology, histopathology, cytopathology, immunoserology, molecular biology.[22]

85. AEL is a regional provider of esoteric and clinical laboratory services, "focused to provide the unique turnaround time and quality demands for testing services for health care providers."[23] AEL uses advanced information technology solutions to automate and streamline electronic assay ordering and result reporting for its customers.

86. AEL is the "MidSouth Division" of Sonic and a subsidiary of Sonic, and provides testing locations in Tennessee include the core laboratory in Memphis and AEL East in Knoxville. Additional AEL laboratories are located in Mississippi, Alabama, Missouri, and Arkansas. AEL also operates convenient patient service centers throughout Alabama, Arkansas, the Florida panhandle, Kentucky, Mississippi, Missouri, and Tennessee.[24]

87. Sunrise, a subsidiary of Sonic, offers a "broad spectrum" of clinical laboratory testing "designed to provide physicians and their patients with the most accurate and diagnostically

---

21 Bloomberg Law, Clinical Pathology Laboratories, Inc., Company Profile, https://www.bloomberglaw.com/company/ticker/610329Z%20US%20Equity; Laboratory Locations, https://www.cpllabs.com/locations/.

22 Pathology Services, https://www.cpllabs.com/about-us/medical-expertise/pathology-services/. CPL works with Pathology Affiliates specializing in the following fields: anatomic, breast, cytopathology, clinical, dermatopathology, gastrointestinal, gynecologic, hematopathology, head and neck, placental, molecular, pediatric, urologic, renal, and transfusion. *See* Pathology Affiliates, https://www.cpllabs.com/about-us/medical-expertise/pathology-affiliates/.

23 *About Us*, American Esoteric Laboratories, https://www.ael.com/about-us/about-ael/ (last accessed Nov. 13, 2019).

24 *Id.*

meaningful results."[25]

88. "CBLPath, a Sonic subsidiary, is a leading diagnostic, molecular and informatics reference laboratory that combines anatomic pathology with advanced molecular diagnostics and multi-platform testing systems."[26] Serving more than 3,900 physician specialists and their patients throughout the United States,[27] CBLPath offers a range of laboratory services, including breast pathology, cytopathology, dermatopathology, general surgical pathology, gastrointestinal pathology, hematopathology, and uropathology.[28]

89. Sonic is the parent company of Defendant CPL as well as its other subsidiaries AEL, Sunrise, and CBLPath. Sonic also provides these subsidiaries with management services.

90. Defendant CPL, as well as AEL, Sunrise, and CBLPath, (collectively "Sonic subsidiaries") entered into two agreements with Sonic that help define the relationship between these Defendants.

91. The first type of agreement each Sonic subsidiary entered into with Sonic is a business associate agreement.

92. HIPAA requires that covered entities[29] enter into contracts with their business

---

25 *About Us*, Sunrise Medical Laboratories, https://www.sunriselab.com/about-us/ (last accessed Nov. 14, 2019).

26 CBLPath, https://www.cblpath.com/home/ (last accessed Nov. 13, 2019).

27 *About Us*, CBLPath, Inc., https://www.cblpath.com/about-us/ (last accessed Nov. 14, 2019).

28 *Specialties,* CBLPath, Inc., https://www.cblpath.com/about-us/our-team/our-pathologists/ (last accessed Nov. 14, 2019).

29 HIPAA defines "covered entities" as health plans, healthcare clearinghouses, and health providers that "transmit[ ] any health information in electronic form in connection with a [covered] transaction." 45 C.F.R. § 160.103.

associates[30] to ensure that the business associates will appropriately safeguard PHI of the covered entities. These contracts are called business associate agreements ("BAAs"). BAAs also serve to clarify and limit, as appropriate, the permissible uses and disclosures of PHI by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate.[31]

93. In the BAAs entered into between Sonic and each of its subsidiaries, Sonic was defined as the "business associate" and the subsidiaries were defined as "covered entities."

94. The subsidiaries also each entered into a Management Services Agreement ("MSA") with Sonic. These MSAs set forth the services Sonic provides for its subsidiaries as their management company.

95. The MSAs state that Sonic provides, amongst other services, "[a]ccess to Information Technology personnel services" to its subsidiaries and provides its subsidiaries "certain administrative services."[32]

96. Defendant Aurora is a wholly-owned subsidiary of Sonic, and is a leading, independent pathology services and cancer diagnostics company, offering integrated diagnostic and personalized medicine consultations and information technology solutions to physicians and hospital systems.

97. Aurora's services include anatomic pathology services, dermatopathology services,

---

30 Under HIPAA, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information. 45 C.F.R. § 160.103.

31 45 C.F.R. § 164.504(e).

32 *See* SONIC0004-0008.

molecular services, and hospital services. To provide these services, Aurora relies upon its owned subsidiaries and partner entities, which provide the services. They include:

a. Laboratory Medicine Consultants provides "custom, accessible, state-of-the-art diagnostic and consultative services to clinicians and their patients."[33] It is the exclusive professional pathology services provider for a number of hospitals in Nevada.[34]

b. Aurora Diagnostics South Texas Dermatology Lab provides dermatopathology services "dedicated to maintaining the utmost care in the diagnosis of skin disease."[35] It provides the "highest quality pathology services," with "the highest standards, while providing unsurpassed services to physicians and their patients."[36]

c. "Aurora Diagnostics Pathology Solutions is a national provider of anatomic pathology services."[37] Priding itself on its association with major academic institutions and a network of subspecialty pathologists, PS says: "Our philosophy is simple: provide a high level of client service, alongside the highest level of expertise and industry-leading turnaround-time, providing unparalleled results!"[38]

d. Aurora Diagnostic Seacoast Pathology "provides the highest quality, customized

---

33 *LMC Pathology Services*, Aurora Diagnostics, https://www.auroradx.com/lmc-pathology-services/ (last accessed Nov. 13, 2019).

34 *Id.*

35 *South Texas Dermatopathology*, Aurora Diagnostics, https://www.auroradx.com/south-texas-dermatopathology/ (last accessed Nov. 12, 2019).

36 *Id.*

37 *Pathology Solutions*, Aurora Diagnostics, https://www.auroradx.com/pathology-solutions/ (last accessed Nov. 14, 2019).

38 *Id.*

pathology services to physicians throughout New England."[39]

e. Aurora Diagnostic Arizona Dermatopathology "is a full-service dermatopathology laboratory that is known for unmatched expertise, specializing in personalized attention to detail and rapid turnaround time."[40] Touting its "expert dermatopathologists," which are "recognized leaders in the field of dermatopathology," AD promises to provide patients with "the most accurate and reliable diagnosis."[41]

f. Aurora Diagnostics Western Pathology Consultants is the "premier provider of outpatient/inpatient anatomic and clinical pathology for Northern Nevada and the Eastern Sierra Nevada communities of California."[42] WPC touts that it provides "superior healthcare through the provision of expert and prompt diagnostic pathology services communicated with clarity" and that it applies "new technologies to support the evolving needs of our clients."[43]

g. Aurora Diagnostics Laboratory of Dermatology provides customized dermatopathology services to dermatologists, general practice physicians, family practice physicians, and podiatrists throughout the State of New York.[44]

---

[39] *Seacoast Pathology*, Aurora Diagnostics, https://www.auroradx.com/seacoast-pathology/ (last accessed Nov. 14, 2019).

[40] *Arizona Dermatopathology*, Aurora Diagnostics, https://www.auroradx.com/arizona-dermatopathology/ (last accessed Nov. 13, 2019).

[41] *Id.*

[42] *Western Pathology*, Aurora Diagnostics, https://www.auroradx.com/western-pathology/ (Nov. 13, 2019).

[43] *Id.*

[44] *Laboratory of Dermatology*, Aurora Diagnostics, https://www.auroradx.com/laboratory-of-dermatopathology/ (last accessed Nov. 13, 2019).

h. Defendant Aurora Diagnostics Austin Pathology provides "expert surgical and clinical pathology diagnostic and consultative services, as well as rapid turnaround and cost-effective delivery of services."[45] It prides itself on the use of "leading-edge laboratory and computer technology" in providing services to patients.[46]

98. Aurora is the parent and management company of Defendant Austin Pathology as well as its other subsidiaries Laboratory Medicine Consultants, South Texas Dermatology Lab, Pathology Solutions, Seacoast Pathology, Arizona Dermatopathology, Western Pathology Consultants, and Laboratory of Dermatology (collectively "Aurora subsidiaries").

99. Aurora entered into MSAs with each Aurora subsidiary. These MSAs set forth the services Aurora provides to each Aurora subsidiary.[47]

100. Aurora provides billing services to each Aurora subsidiary. Aurora bills the patients of each Aurora subsidiary and collects the professional and ancillary fees for all medical and professional services rendered by each Aurora subsidiary. Each Aurora subsidiary also appointed Aurora to be its true and lawful attorney-in-fact to bill patients and to collect accounts receivable resulting from such billing in the Aurora subsidiary's name and on its behalf.[48]

101. Aurora provides "Record Management" services to each Aurora subsidiary. Aurora maintains all files and records of each Aurora subsidiary relating to the operation of the Aurora subsidiary or the practice of medicine by the Aurora subsidiary, including accounting, billing,

---

45 *Austin Pathology*, Aurora Diagnostics, https://www.auroradx.com/austin-pathology/ (last accessed Nov. 14, 2019).

46 *Id.*

47 *See* SONIC0009-00027.

48 *Id.*

collection and customary financial records, and patient files.[49]

102. Aurora provides "General Administrative Services" to each Aurora Lab to relieve these labs to "the maximum extent possible" of the administrative, accounting, purchasing, non-physician personnel and other business aspect of each Aurora subsidiary's medical practices.[50]

103. Additionally, the services Aurora provides to each Aurora subsidiary are not constrained to those listed in the MSAs. For example, Aurora provides the Aurora subsidiaries with HIPAA-related policies. Aurora created the "Aurora HIPAA Manual," which applies to all Aurora subsidiaries.[51] The Aurora Legal Department also advises Aurora subsidiaries about pursuing certain patient accounts for collections.[52]

104. Upon information and belief, Defendants Sonic, Aurora, CPL, and Austin Pathology, as well as Sonic and Aurora's other subsidiaries, charge patients for the laboratory services provided to them and their invoices include only fees for such services. Patients are responsible for paying Defendants for performing diagnostic services either through their insurance or out-of-pocket, if the patient does not have insurance or the costs are not entirely covered by insurance.

105. Patients who received laboratory services from a Sonic subsidiary pay for those services through a website maintained by Sonic located at https://payments.sonichealthcareusa.com.

106. After patients made a payment through Sonic's website for laboratory services that

---

49 *Id.*

50 *Id.*

51 *See* SONIC00563-94; SONIC01118-1129.

52 *See* AMCAPROD00940840.

they received from a Sonic subsidiary, those patients receive a billing confirmation email from a "sonichealthcareusa.com" email address.

107. In addition to maintaining the patient billing website for the Sonic subsidiaries, employees of Sonic communicated with patients of the Sonic subsidiaries who contested bills for laboratory services.

108. Patients who received laboratory services from Aurora subsidiaries pay for those services through a website maintained by Aurora called https://www.auroradx.com/online-bill-pay/.

109. As a part of the billing services Aurora provided for its subsidiaries, Aurora employees communicated with patients of its subsidiaries who contested bills for laboratory services.

110. If Defendants' patients as well as the patients of the subsidiaries of Defendants, fail to pay their invoices within the requested time period, Defendants employ an associated business for collection. During the relevant time period, Defendants utilized AMCA as a billing collection agency.[53]

111. Sonic and Aurora Diagnostics directed the use of AMCA as the standardized billing collections vendor for all their subsidiaries impacted by the Data Breach.

112. At Sonic's direction, the subsidiaries of Sonic each entered into a BAA with AMCA.

113. Aurora entered into a BAA with AMCA on behalf of all of its subsidiaries.

---

[53] *Clinical Pathology Laboratories, Inc. Notifies Patients of Data Security Incident*, Clinical Pathology Laboratories, (July 12, 2019), https://www.cpllabs.com/about-us/announcements/?q=incident.

114. Upon information and belief, Sonic did not have a BAA with AMCA.

115. In order to facilitate the collection of invoices, Sonic and its subsidiaries provided AMCA with its patients' Personal Information, which AMCA in turn stored in its own computer systems. In addition, as part of AMCA's billing collection services for Defendants, Plaintiffs furnished Personal Information directly to AMCA, which AMCA subsequently stored.

116. Although Sonic is the parent and management company of its subsidiaries, Sonic directly interacted with AMCA on behalf of its subsidiaries.

117. Sonic provided AMCA with the Personal Information of the patients of its subsidiaries CPL, AEL, CBLPath, and Sunrise, including, but not limited to dates of birth, address, Social Security numbers, email addresses, and even medical information such as patient identification numbers, diagnosis codes, diagnostic testing codes, medical insurance information, and physician information.[54]

118. For example, a Sonic accounts receivable specialist, Phyllis Cordova, frequently emailed Erika Almonte, a Legal/Compliance Assistant at AMCA, "Patient Inquiry" forms and "Housekeeping Reports" for AEL and CPL patients.

119. On October 22, 2018, Cordova emailed a Patient Inquiry form for an AEL patient to Almonte. This form included the fully unredacted social security number, date of birth, address, phone number, patient identification number, and medical testing information of that patient.

120. On December 18, 2018, Cordova emailed Almonte a Housekeeping Report of a CPL patient. This report included the date of birth, address, physician information, insurance information, medical history, and diagnosis codes of the patient.

---

[54] *See, e.g.*, AMCAPROD00234672; AMCAPROD00234760; AMCAPROD00908309.

121. Upon information and belief, Sonic provided AMCA with the Personal Information of Sonic Divisions' patients without entering into a BAA with AMCA.

122. Sonic was able to provide AMCA with the Personal Information of the Sonic Divisions' patients because Sonic had access to those patients' Personal Information in Sonic's own computer systems.

123. For example, Cordova stated in an October 8, 2018 email to Almonte that she could access a CPL patient's account in Sonic's computer system.

124. Additionally, on April 4, 2017, Sonic developer, Mauli Desai, emailed AMCA's Director of IT & Security, Zak Raxter, a screenshot of his computer screen. The screenshot showed that Sonic had a "Site Manager" program that contained an "AMCA_InFolder" as well as several subfolders. Those subfolders were named for Sonic Divisions such as CPL, CBLPath, and AEL. The correspondence indicates these subfolders named for CPL, CBLPath, and AEL contain the patients' collection files of those Sonic subsidiaries that were to be sent to AMCA for collection purposes.

125. Sonic provided AMCA with "patient accounts," "weekly collections file," and "AMCA Transaction Forms," all containing the Personal Information of the patients of the Sonic Divisions, on behalf of Sonic Divisions.[55]

126. For example, Christopher Bain and Larry Johnson, employees of Sonic, emailed AMCA "weekly collection files." These files provided AMCA with the Personal Information of Sonic Division patients in order for AMCA to perform its collection services on behalf of Sonic and its subsidiaries.

---

[55] *See, e.g.*, AMCAPROD00672763; AMCAPROD00669737; AMCAPROD00002036.

127. Sonic also communicated with AMCA on behalf of Sonic Divisions to resolve IT issues.

128. For example, Sonic employees Mauli Desai, Wednesday Tijerina, William Rodriguez, Jeff DeFreitas, and Armando Zubin frequently communicated with AMCA on behalf of labs about IT issues such as server connection errors encountered by Sonic and its subsidiaries when Sonic or its subsidiaries Defendants attempted to send patient collection files to AMCA.

129. Additionally, Sonic negotiated collections rates for AMCA's services on behalf of its subsidiaries. For example, in a February 19, 2019 email, AMCA's director, David Ulrich, acknowledged that all "Sonic locations" had a 19% collections rate.

130. In order to facilitate the collection of invoices, Aurora and its subsidiaries also provided AMCA with its patients' Personal Information, which AMCA in turn stored in its own computer systems. In addition, as part of AMCA's billing collection services for Defendants, Plaintiffs furnished Personal Information directly to AMCA, which AMCA subsequently stored.

131. Aurora interacted with AMCA on behalf of its subsidiaries to facilitate the collection of invoices.

132. Aurora directly, or through its billing vendors Change Healthcare and McKesson Corporation, provided AMCA with the Personal Information of its subsidiaries' patients, including but not limited to patients' Social Security numbers, phone numbers, addresses, and dates of birth, in monthly collection files also known as "placement files."[56]

133. For example, on November 22, 2016, Aurora's Regional Billing Manager, Carolyn Lange, emailed Pathology Solutions', a subsidiary of Aurora, collections file to AMCA for

[56] *See, e.g.*, AMCAPROD00693961; AMCAPROD00000654; AMCAPROD00000654.

October 2016. The file contained patients' addresses, dates of birth, telephone numbers, insurance policy names and numbers, the last four digits of Social Security numbers, and physicians' information.[57]

134. Aurora controlled any payments between AMCA and its subsidiaries. For example, when AMCA collected money from the patients of Aurora's subsidiaries, AMCA would not transfer that money directly to the respective Aurora subsidiaries but would deposit the money into Aurora's bank accounts.[58]

135. Aurora controlled AMCA's "collection rate" for each Aurora Lab. For example, in a September 27, 2016 email, Carolyn Lange, Aurora Diagnostics Regional Billing Manager, informed David Ulrich, Director of AMCA, that the collection rate for "all Aurora Sites" serviced by AMCA would change from 24% to 22%.[59]

136. Aurora was responsible for addressing any billing issues that AMCA encountered in connection with Aurora's subsidiaries. For example, in an April 13, 2018 email from Aurora employee, Alison Ford, to AMCA employee, Marlene Ellington, Ford directed Ellington to contact Aurora employees Nicole Mason, Malinda Hill, Bernadine Rowlands, or Carolyn Lange for billing issues concerning Aurora subsidiaries including Defendant Austin Pathology.[60]

C. How the Data Breach Occurred.

137. From at least August 1, 2018 and March 30, 2019, an unauthorized user or users gained access to the AMCA system that contained information obtained from various entities,

---

57 *See* AMCAPROD00267121.

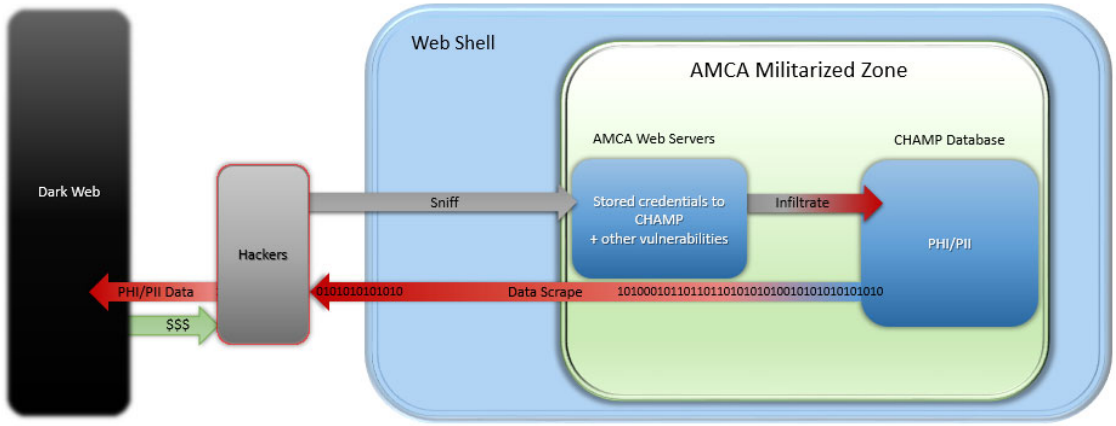
58 *See, e.g.*, AMCAPROD00693866-693870; AMCAPROD00694040-694042.

59 *See* AMCAPROD00427755.

60 *See* AMCAPROD00915840.

including Defendants, as well as information that AMCA collected itself. This date range is limited by the scope of AMCA's investigation and AMCA's lack of historical logging and monitoring of activity on its systems, and the intrusion may have covered a longer period.

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



139. Prior to the discovery of the Data Breach, AMCA was alerted by Nuvei (a payment processor) of a potential compromise of credit cards processed by AMCA. This alert prompted AMCA to hire EndPoint Corporation, a software development and hosting provider, to perform an audit. End Point's audit found the presence of malicious scripts, outdated software, security and privacy settings that were below industry standard, and a lack of compliance with the PCI-DSS standards and HIPAA.

140. After the Data Breach was discovered, Charles River Associates, a consulting firm

engaged by AMCA, provided a "forensic analysis" of the AMCA system after the Data Breach was discovered. Charles River conducted a limited investigation and nevertheless concluded that [redacted][61]

141. Specifically, the evidence shows that [redacted][62] Webshells are pieces of code placed on a web application server to provide an interface for a remote attacker to execute commands. An attacker attaches an executable script, here in the PHP coding language, to the web server and the script searches for vulnerabilities in a web server's systems. The web shell can also execute commands and upload and download files.

142. Web shells are only possible if the web application or server contain vulnerabilities such as insecure or poorly written code, a misconfiguration, credentials that are unencrypted, a lack of security patching, or minimal segmentation between different areas in a network. Moreover, web shells leave contemporaneous evidence of their activities, referred to as "noise," but AMCA did not capture this because it was not logging the traffic on its web servers and it did not employ a Web Application Firewall. Additionally, commercial scanning tools and anti-virus software can detect and prevent the installation of web shells, but AMCA did not employ them here.

143. By installing the webshell, threat actors were able to gain access to AMCA's consumer database and possibly the entire organization's network.

144. From there, they were able to exploit the unpatched and out-of-date AMCA IT

[61] [redacted] (emphasis added).

[62] *Id.*

systems to perpetrate the Data Breach.

145. Specifically, threat actors found numerous vulnerabilities within AMCA's systems. the following [redacted]:[63]

[redacted]

146. These security vulnerabilities existed because AMCA's web servers used systems that were out of date, unpatched, untested, and were not "hardened," i.e., fortified using appropriate security measures. AMCA ran an unsupported and vulnerable version of PHP, an open-source coding language. As an EndPoint security review acknowledged in a March 2019 report to AMCA, there was a need to "upgrade to latest PHP." In March 2020, amcaonline.com still showed an unpatched version of Apache and an unpatched version of MySQL.

147. Further, AMCA failed to patch and upgrade its IT systems. This is a basic feature of IT security. It is well known in the industry that threat actors learn of vulnerabilities in IT

[63] RMCB-AG-195, at 3-4.

systems and exploit them if they are not patched, and even basic IT security requires constant patching and updating as potential vulnerabilities become known. Further, because AMCA's web server was publicly available on the Internet, attackers could scan it and learn that it utilized unpatched and out-of-date software.

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

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

a. AMCA was not running an antivirus scanner or a scan of its file system to detect known malware; and

b. AMCA's Security Information and Event Management (SIEM) was not logging activities on its servers.

150. Even if an attacker is able to gain access to AMCA's systems via a webshell, an appropriate IT system needs to provide additional layers of security to protect the most important (and desirable) information. This includes segregating the most important systems from less essential systems and limiting access to these systems. For AMCA, the CHAMP database stored Defendants' patient PII/PHI and was the most important system to protect. Information contained in the CHAMP database included:

- Patient names
- Patient addresses
- Patient contact phone numbers (up to three)
- Patient Social Security numbers
- Patient dates of birth
- Guarantor/responsible party names

- Guarantor/responsible party name addresses
- Guarantor contact phone numbers (up to three)
- Guarantor / responsible party Social Security numbers
- Subscriber member
- Referring physician name
- Insurance designation flag
- Insurance group number and insurance ID
- Medicare / Medicaid number
- Patient/subscriber account number
- Specimen collection date
- Dates of service
- Specimen number
- Patient ID
- Invoice/requisition numbers
- Clinical information
- International Classification of Diseases Diagnosis and Procedure Codes ("ICD Codes") and diagnosis codes
- Test order names
- Test order results
- Photographs taken for paternity identity testing

151. However, instead of providing additional security to the CHAMP database, AMCA left the CHAMP database accessible to the internet. Additionally, the CHAMP database was supposed to be segregated from the remainder of AMCA's IT system but was not.

152. In practice, what this meant was that once threat actors gained access to AMCA's systems they could traverse from the web server to the CHAMP database. This was made even easier by the fact that AMCA left stored credentials (i.e., user name and passwords) accessible ***and*** threat actors could override the system's requirement to enter authorizations to access the CHAMP database.

153. The Charles River timeline reveals that once threat actors entered the AMCA system as early as August 1, 2018, without detection, they were able to "sniff and scrape"—i.e.

monitor what was going on in system ("sniff") and wipe away their tracks after exfiltrating information ("scrape"). [redacted][64]

154. [redacted][65] Specifically, threat actors downloaded files related to collection letters, access lists, credentials, a list of transactions, among other things.

155. On January 27, 2019, threat actors were able to insert another webshell without detection.

156. On March 11, 2019 and March 29, 2019, threat actors downloaded several files from AMCA without detection. Specifically, threat actors exfiltrated 14 files on March 11, 2019 that included access lists and user credentials. And on March 29, 2019, threat actors exfiltrated another 40 files.

157. At no point did AMCA discover the threat actors—not upon entry, not when they traversed the system, not when they overrode the requirement for user authentication, and not when they exfiltrated files.

D. AMCA's 2019 Audit Revealed Serious Vulnerabilities that it did not remediate.

158. EndPoint's March 2019 audit of AMCA revealed numerous un-remediated deficiencies. First, AMCA was using a Linux operating system that had not been updated or patched and was relying on a 2015 version of software.

[64] RMCB-AG-195.

[65] *Id.* at 2.

159. Further, the production database server had no network segmentation between the publicly exposed web server and the underlying database. AMCA also failed to follow recommended security practices on its MySQL program. In layman's terms, this meant that compromising the public-facing web server allowed threat actors to compromise the underlying, non-public facing, database server containing the PII and PHI at issue in this case.

160. EndPoint also had to upgrade AMCA's firewall policies and discovered malicious scripts on AMCA's webserver. EndPoint could not even tell how long malicious, undetected scripts had been present because AMCA did not have the requisite Web Application Firewall installed and was not logging traffic on the web server. EndPoint had to remediate both of these deficiencies, in addition to installing an antivirus scanner and new rules and controls to prevent SQL injections.

161. During this same period, available network logs showed that a keylogger, a program that tracks what keys are pressed, was installed on a Mac device in AMCA's finance/accounting department since March 7, 2018, seven months before evidence of a web shell was found on the web server. The keylogger made multiple successful connections to an external IP address. The user who operated the Mac device worked in AMCA's finance department and thus had access to its accounting system that processed credit card payments. The End Point auditor wrote: "we should make the assumption that someone could've obtained any passwords typed into this machine and potentially any data on it." And "the fact that they were able to run code, means they could've ran anything they wanted, so yes, they could've obtained full access to that Mac, and moved laterally through the network to anything else connected."

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

163. Specifically in November 2018, after forensic evidence proved that files were exfiltrated by threat actors, AMCA was contacted by GlobalOnePay who informed AMCA that [redacted][66] This was done via a "common point of purchase" which is a way for credit cards issuing banks to trace fraud associated with the use of their cards.

164. At that time, Conformance Tech noted that there were a "small number of cards [that had fraud on them], BUT, it is from a really small card issuer. Small banks and Discover [credit cards] tend to be leading indicators of larger problems."[67]

165. In response, AMCA conducted an internal review and concluded that no one had accessed credit card data from its systems because there was "evidence of this shown in our exhaustive review."[68]

166. On February 13, 2019, AMCA was again contacted by GlobalOnePay about another common point of payment ("CPP") alert involving fraud on 22 credit cards.[69] AMCA again took the position that there had not been a data breach.

167. On February 25, 2019, AMCA was informed by Nuvei, a payment technology partner, that New York Community Bank informed it that 88 credit cards were breached between December 26, 2017 and December 17, 2018.[70]

---

[66] RMCB-AG-25.

[67] AMCAPROD138907.

[68] *Id.*

[69] AMCAPROD0215349.

[70] AMCAPROD1117103.

168. At the end of February 2019, Gemini Advisory, a New York-based company that works with financial institutions to monitor the sale of consumer information on underground markets, ***identified a large number of compromised AMCA patient information for sale on the dark web***.[71] As reported on May 10, 2019, by DataBreaches.net:

> On February 28, 2019, Gemini Advisory identified a large number of compromised payment cards while monitoring dark web marketplaces. Almost 15% of these records included additional personally identifiable information (PII), such as dates of birth (DOBs), Social Security numbers (SSNs), and physical addresses. A thorough analysis indicated that the information was likely stolen from the online portal of the American Medical Collection Agency (AMCA), one of the largest recovery agencies for patient collections. Several financial institutions also collaboratively confirmed the connection between the compromised payment card data and the breach at AMCA.[72]

169. Gemini's additional research revealed AMCA's exposure window had lasted for at least seven months beginning in September 2018.[73]

170. The combination of AMCA-related PII being for sale on the dark web and the cpp notifications that AMCA received definitively shows that the threat actors, after exfiltrating PII and PHI from AMCA's systems, selling the information on the dark web and purchasers of that information were subsequently committing credit card fraud.

171. "On March 1, 2019, Gemini Advisory attempted to notify AMCA," but, as Gemini Advisory reportedly told DataBreaches.net, "they did not get any response to phone messages they

---

71 Gemini Advisory, *AMCA Breach May be Largest Medical Breach in 2019* (June 4, 2019), available at https://geminiadvisory.io/amca-largest-medical-breach/ (last visited Mar. 21, 2022).

72 Databreaches.net, *American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory* (posted May 10, 2019), available at https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/ (last visited Mar. 21, 2022).

73 *Id.*

left."[74] Failing to obtain any response from AMCA, Gemini Advisory "promptly contacted federal law enforcement, which reportedly followed up by contacting AMCA."[75]

172. Following notification from law enforcement, AMCA's payment portal became unavailable for weeks.[76]

173. In a written statement attributed to AMCA in June, at the time, AMCA announced it was still investigating the breach:

> We are investigating a data incident involving an unauthorized user accessing the American Medical Collection Agency system," reads a written statement attributed to the AMCA. "Upon receiving information from a security compliance firm that works with credit card companies of a possible security compromise, we conducted an internal review, and then took down our web payments page.
>
> . . . .
>
> We hired a third-party external forensics firm to investigate any potential security breach in our systems, migrated our web payments portal services to a third-party vendor, and retained additional experts to advise on, and implement, steps to increase our systems' security. We have also advised law enforcement of this incident. We remain committed to our system's security, data privacy, and the protection of personal information.[77]

174. There are strong indications that the information exfiltrated from AMCA's database is still being offered for sale on underground markets. An expert recently compiled the information of more than 60 individuals from varying geographic regions and demographics who had their information stored on AMCA's database and searched for their information on dark web markets

---

74 *Id.*

75 *Id.*

76 *Id.*

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

notorious for selling confidential personal information acquired from threat actors and malicious threat actors. The expert discovered that more than 87% of the sample population had their information offered for sale by *two single vendors* on one popular dark web market. It is highly unlikely that information associated with such a significant percentage of the sample would be available through two vendors unless the data was obtained from the same breach—providing strong evidence that all class members had their information accessed, exfiltrated, and then disseminated by unauthorized parties.

E. Sonic and Aurora's patients' information was exposed in the Data Breach.

175. Millions of Defendants' patients were affected by the Data Breach—including nearly 2 million CPL patients, 7,400 AEL patients,[78] 15,000 Sunrise patients,[79] 3,800 CBLPath patients,[80] 4,200 LMC patients,[81] 1,200 South Texas Dermatopathology patients,[82] 600 Pathology

[78] PR Newswire, *American Esoteric Laboratories Notifies Patients of Data Security Incident*, (July 15, 2019), https://www.prnewswire.com/news-releases/american-esoteric-laboratories-notifies-patients-of-data-security-incident-300885206.html.

[79] PR Newswire, *Sunrise Medical Laboratories, Inc. Notifies Patients of Data Security Incident* (July 15, 2019), https://www.prnewswire.com/news-releases/sunrise-medical-laboratories-inc-notifies-patients-of-data-security-incident-300885210.html.

[80] PR Newswire, *CBLPath, Inc. Notifies Patients of Data Security Incident* (July 15, 2019), https://www.prnewswire.com/news-releases/cblpath-inc-notifies-patients-of-data-security-incident-300885213.html.

[81] PR Newswire, *Laboratory Medicine Consultants, Ltd. Notifies Patients of Data Security Incident* (July 19, 2019), https://www.prnewswire.com/news-releases/laboratory-medicine-consultants-ltd-notifies-patients-of-data-security-incident-300888273.html.

[82] PR Newswire, *South Texas Dermatopathology, PLLC Notifies Patients of Data Security Incident* (July 19, 2019), https://www.prnewswire.com/news-releases/south-texas-dermatopathology-pllc-notifies-patients-of-data-security-incident-300888271.html.

Solutions patients,[83] 800 Seacoast patients,[84] 500 AD patients,[85] 350 Western Pathology patients,[86] 240 LDA patients,[87] and 1,800 Austin Pathology patients,[88] —making it one of the largest health-related data breaches reported to the U.S. Department of Health and Human Services ("HHS") in 2019.[89] The overall AMCA Data Breach (including all impacted laboratories) was the second largest to be reported since HHS's Office for Civil Rights launched its breach portal in 2010.[90]

176. Sonic and Aurora were notified of the AMCA breach through its subsidiaries on May 15, 2019, two months before Sonic and Aurora's subsidiaries began to give notice of the data

---

[83] PR Newswire, *Pathology Solutions, LLC Notifies Patients of Data Security Incident* (July 19, 2019), https://www.prnewswire.com/news-releases/pathology-solutions-llc-notifies-patients-of-data-security-incident-300888268.html.

[84] PR Newswire, *Seacoast Pathology, Inc. Notifies Patients of Data Security Incident* (July 19, 2019), https://www.prnewswire.com/news-releases/seacoast-pathology-inc-notifies-patients-of-data-security-incident-300888267.html.

[85] PR Newswire, *Arizona Dermatopathology Notifies Patients of Data Security Incident* (July 19, 2019), https://www.prnewswire.com/news-releases/arizona-dermatopathology-notifies-patients-of-data-security-incident-300888270.html.

[86] PR Newswire, *Western Pathology Consultants, Ltd. Notifies Patients of Data Security Incident* (July 19, 2019), https://www.prnewswire.com/news-releases/western-pathology-consultants-ltd-notifies-patients-of-data-security-incident-300888272.html.

[87] PR Newswire, Laboratory of Dermatopathology ADX, LLC Notifies Patients of Data Security Incident (July 19, 2019), https://www.prnewswire.com/news-releases/laboratory-of-dermatopathology-adx-llc-notifies-patients-of-data-security-incident-300888266.html.

[88] PR Newswire, *Austin Pathology Associates Notifies Patients of Data Security Incident* (July 19, 2019), https://www.prnewswire.com/news-releases/austin-pathology-associates-notifies-patients-of-data-security-incident-300888265.html.

[89] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,* U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited October 9, 2019); *see also August 2019 Healthcare Data Breach Report*, HIPAA Journal, https://www.hipaajournal.com/august-2019-healthcare-data-breach-report/ (last visited October 9, 2019).

[90] *July-reported healthcare breaches exposed 22 million people's data*, Modern Healthcare, https://www.modernhealthcare.com/cybersecurity/july-reported-healthcare-breaches-exposed-22-million-peoples-data (last visited Oct. 9, 2019).

Breach to their patients.

177. On June 5, 2019, Sonic directed its subsidiaries, including the Sonic subsidiaries, Aurora, and Aurora's subsidiaries to stop sending patient files to AMCA.[91]

178. Each Defendant publicly announced that patient names, phone numbers, dates of birth, dates of service, balance information, credit card or banking information, and treatment provider information were exposed by the Data Breach.[92]

179. According to Defendants' announcements,[93] AMCA became aware of the Data Breach on March 21, 2019, and notified the Defendants in May 2019 that information for some of their patients had been exposed in the Data Breach.

180. The Defendants have advised the United States Department of Health and Human Services Office for Civil Rights ("OCR") of the Data Breach.[94]

181. Sonic also "coordinated" its own investigation into the Data Breach "at the corporate parent level" for its subsidiaries, including Defendants CPL and Aurora, as well as Defendant Austin Pathology and Aurora's other subsidiaries.[95]

II. Defendants failed to provide proper notice of the Data Breach.

182. Although Defendants were on notice of the Data Breach in May 2019 (and should have known months earlier), it took them approximately a month and a half to publicly acknowledge the Data Breach, and it appears that only a fraction of impacted customers have been

---

91 *See* SONIC00779-791; SONIC2809-2824.

92 *See* ¶ 71, *supra.*

93 Sonic and Aurora did not make public announcements.

94 *Cases Currently Under Investigation*, U.S. Department of Health and Human Services Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

95 *See* SONIC02809-2824.

notified.

183. Defendants publicly acknowledged the Data Breach in mid-July 2019, but have not publicly confirmed that they sent direct notice of the Data Breach to patients.[96] For example, on July 15, 2019, CPL reported that "AMCA sent notification letters to approximately 34,500 CPL patients" and "that approximately another 2.2 million patients may have" been impacted by the Data Breach, but CPL has been silent with respect to its efforts to communicate directly with patients.[97]

184. It appears that Defendants have failed to provide proper notification to millions of Class Members that their Personal Information may have been compromised.

185. Defendants' failure to properly disseminate notice further harmed their customers by keeping them in the dark about whether they were affected by the Data Breach and how they could quickly and safely respond.

III. Defendants committed to safeguarding their patients' personal information, and that commitment emanates from the control that Sonic has over them.

186. As stated herein (§ I.A), Sonic's and Aurora's commitment to patient privacy was reinforced through their agreements with vendors, doctors, suppliers, agents, and subsidiaries. The rest of the Defendants were no exception.

187. Sonic had authority, through its Foundation Principles, Values, and agreements, to ensure that its subsidiaries, wholly-owned entities, partner organizations, hospitals, doctors, and

---

96 *Clinical Pathology Laboratories, Inc. Notifies Patients of Data Security Incident*, Clinical Pathology Laboratories, (July 12, 2019), https://www.cpllabs.com/about-us/announcements/?q=incident.

97 *Clinical Pathology Laboratories, Inc. Notifies Patients of Data Security Incident*, PR Newswire, (July 15, 2019), https://www.prnewswire.com/news-releases/clinical-pathology-laboratories-inc-notifies-patients-of-data-security-incident-300885218.html.

laboratories maintained a level of confidentiality of patient Personal Information. Accordingly, Sonic dictated privacy practices, and its subsidiaries Defendant CPL, as well as CBLPath, Sunrise, and AEL were required to follow them.

188. Similarly, Aurora's subsidiaries dictated privacy practices for all of its subsidiaries.

189. Defendants CPL and Austin Pathology, as well as Sonic's and Aurora's other subsidiaries, in turn, acknowledged their responsibility to keep patient information confidential. For example, CPL's website states that it, like all Sonic healthcare companies, possesses "a deep understanding of the special complexities, obligations and privileges of medical practice,"[98] and is committed to a "set of core values" that includes "keep[ing] all information pertaining to patients . . . in strict confidence."[99]

190. In addition, HIPAA requires that Defendants provide every patient they treat, including Plaintiffs and the putative Class Members, with a privacy notice. In CPL's Notice of Privacy Practices for Protected Health Information, CPL states as follows:

We are Required to:

- Maintain the privacy and security of your health information
- Inform you if a breach occurs that may have compromised the privacy or security of your information

---

98 *Medical Leadership*, Clinical Pathology Laboratories, Inc., https://www.CPL.com/about-us/the-sonic-healthcare-difference/medical-leadership/.

99 *Our Values*, Clinical Pathology Laboratories, Inc., https://www.CPL.com/about-us/the-sonic-healthcare-difference/our-values/. *See also Privacy Policy*, Aurora Diagnostics https://www.auroradx.com/privacy-policy/ ("Aurora Diagnostics believes that privacy is important to the success and use of the Internet.").

- Provide you with a notice of our legal duties and privacy practices regarding the information we collect and maintain about you
- Abide by the terms of this notice
- Notify you by mail, upon your request, if CPL's health information practices change
- Obtain your written authorization for any uses or disclosures of your health information not described in this notice.[100]

191. Defendants also acknowledge that they are required to notify patients in the event of a data breach. For example, CPL states that it "is required to provide patient notification if it discovers a breach of unsecured PHI unless there is a demonstration, based on a risk assessment, that there is a low probability that the PHI has been compromised."[101] A CPL patient "will be notified without unreasonable delay and no later than 60 days after discovery of the breach."[102]

192. Defendants' privacy policies—like Sonic's and Aurora's—indicate that they may provide PHI to companies that assist with billing and to an outside collection agency to obtain

---

100 Clinical Pathology Laboratories, Notice of Privacy Practice for Protected Health Information (PHI) (Oct. 6, 2014), https://www.cpllabs.com/media/3796/notice_of_privacy_practices.pdf?q=notice%20of%20privacy%20practice (emphasis original). The HIPAA notices for the other defendants are substantially similar. *See, e.g.,* Aurora Diagnostics' Notice of Privacy Practices, https://www.auroradx.com/wp-content/uploads/2019/08/HIPAA_Notice_of_Privacy_Practices_ADA.pdf (last accessed Nov. 14, 2019); Sunrise Patient Privacy, https://www.sunriselab.com/patients/patient-privacy/ (last accessed Nov. 15, 2019).

101 *Id.*

102 *Id.*

payment when necessary.[103] These companies are known as "business associates" and are "*required*" to maintain the privacy and security of PHI.[104]

193. The requirements, which stem from contractual duties as well as duties under HIPAA, were violated. Defendants failed to maintain the privacy and security of patients' PHI, failed to ensure that their vendors had the capacity to and would protect patients' PHI, and failed to inform patients that their Personal Information was disclosed.

IV. Defendants failed to exercise due care.

194. AMCA's bankruptcy filings indicate how thinly capitalized the company was and how insignificant its information technology ("IT") department and infrastructure were. Public reporting has suggested that AMCA was not a reputable or stable business associate—let alone an associate to be trusted with Class Members' Personal Information.

195. Specifically, AMCA's bankruptcy filings acknowledge that AMCA had less than $4 million in liquidity and its owner had to take a secured loan from his own personal money simply to mail notices to those impacted by the Data Breach. Put simply, Defendants should not have contracted with an entity that did not even have the means to mail notices to Data Breach victims without having to file for bankruptcy.

196. The length of time between the Data Breach and AMCA's claimed discovery of the Data Breach indicates that AMCA's systems to detect intrusion, detect unusual activity, and log and report such events were woefully inadequate and not in compliance with industry standards. For example, according to technology-security company FireEye, the median amount of time

---

103 *Id.*

104 *Id.* (emphasis added). Aurora Diagnostics' privacy policy is similar: "All of Aurora's Business Associates are required to safeguard the privacy of your PHI."

between when a data breach occurs and when it is detected was 78 days in 2018. This number has consistently been on a downward trend in recent years due to improvements in detection computer technology.[105] The fact that it took AMCA 242 days to detect the Data Breach, nearly 3.5 times the median time for detection in 2018, is direct evidence of its failure to employ reasonable, industry-standard data security practices to safeguard Plaintiffs' and Class Members' Personal Information. AMCA's data security deficiencies would have been apparent had Defendants adequately conducted due diligence on AMCA's data security practices before providing AMCA with their patients' sensitive PHI and PII.

197. AMCA's inability to detect its own Data Breach, when an unrelated security firm (Gemini Advisory, which was not working for AMCA) was apparently able to do so with ease, is further evidence of the fact that AMCA employed inadequate data-security practices, and that Defendants failed in their independent obligations to ensure that its HIPAA business associate employed reasonable and industry-standard data security measures. The FireEye report indicates that in 2018, the median amount of time that it took a third-party (like Gemini Advisory) to detect a data breach was three times the median time for internal detection.[106]

198. AMCA did not need access to Plaintiffs' PHI to collect payments. Instead, AMCA only needed the name of the vendor (Defendants and their subsidiaries), the invoice number, amount owed, and date of service to perform its collection services. But Defendants nevertheless regularly provided full account information that included PHI, apparently because it was more expedient than providing the narrower data set to AMCA.

---

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

106 *Id.*

199. AMCA maintained PHI and PII for closed files and failed to routinely destroy or archive inactive records. Defendants would have discovered this had they exercised adequate oversight over their business associate, AMCA, and audited the data security protocols utilized by AMCA.

200. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). AMCA was not encrypting payment card information according to minimum industry standards of PCI DSS.

201. The payment card industry has published a guide on point-to-point encryption and its benefits in securing payment card data: "point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[107]

202. Defendants had an obligation to exercise oversight over AMCA in a manner that would include immediate knowledge of any data security incidents experienced by AMCA that could affect Defendants' 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

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

portal were later associated with fraudulent charges." However, Defendants did not learn of the unauthorized access until months later in at least May 2019.

203. Defendants agreed, and had continuing contractual and common-law duties and obligations, to keep confidential, the Personal Information its patients disclosed to them and to protect this information from unauthorized disclosure. Defendants' agreements, duties, and obligations are based on: (1) HIPAA; (2) industry standards; (3) the agreements and promises made to Plaintiffs and Class Members; and (4) Section 5(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §45. Class Members provided their Personal Information to Defendants with the reasonable expectation that Defendants and their business associates would comply with their agreements and any legal requirements to keep their Personal Information confidential and secure from unauthorized disclosure.

204. HIPAA requires that Defendants provide every patient they treat, including Plaintiffs and Class Members, with a privacy notice.

205. As described herein, Defendants' privacy notices informed Plaintiffs and Class Members that the Defendants would safeguard and protect PII and PHI, and that Defendants could only use or share PHI for specific purposes.

206. As alleged above, AMCA was a "business associate" of Defendants with whom Defendants shared Personal Information of their patients. As Defendants' business associate, AMCA was required to maintain the privacy and security of Plaintiffs' and Class Members' Personal Information. HIPAA mandates that a covered entity (*i.e.*, Defendants) may 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.[108] Defendants failed to ensure that its business associate AMCA safeguarded Personal Information of Defendants' patients and that AMCA complied with HIPAA's privacy mandates.

V. Defendants violated HIPAA's requirements to safeguard data.

207. Defendants had non-delegable duties to ensure that all information they collected and stored was secure, and that any associated entities with whom they shared member information maintained adequate and commercially-reasonable data security practices to ensure the protection of plan members' Personal Information.

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

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

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

---

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

211. HIPAA requires that Defendants implement appropriate safeguards for this information.

a. HIPAA further mandates that covered entities such as Defendants 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.[109]

b. HIPAA requires that Defendants provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—*i.e.,* non-encrypted data.

212. Despite these requirements, Defendants failed to comply with their duties under HIPAA and their own Privacy Practices. Indeed, Defendants failed to:

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

b. Adequately protect Plaintiffs' and the Class Members' Personal Information;

a. 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);

---

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

b. 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);

c. 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);

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

e. 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);

f. Take safeguards to ensure that Defendants' business associates adequately protect protected health information;

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

h. 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).

213. Additionally, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal

Trade Commission ("FTC") has issued numerous guides for businesses highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[110]

214. The FTC's publication *Protecting Personal Information*: A Guide for Business sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data. Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[111]

215. Additionally, the FTC recommends that organizations limit access to sensitive data, re-quire complex passwords to be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[112]

216. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or

---

[110] FTC, *Start With Security: A Guide for Businesses,* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 21, 2022).

[111] *Id.*

[112] *Id.*

practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[113]

217. Defendants were fully aware of their obligation to implement and use reasonable measures to protect the PHI and PII of Defendants' patients and the patients of their subsidiaries but failed to comply with these basic recommendations and guidelines that would have prevented the Data Breach from occurring.

VII. Defendants were on notice that highly-valuable personal information of their patients could be breached.

218. Defendants were, or should have been, aware that they were collecting highly valuable data, for which Defendants knew, or should have known, there is an upward trend in data breaches in recent years.[114] Accordingly, Defendants were on notice of the harms that could ensue if they failed to protect patients' data.

219. HHS' Office for Civil Rights currently lists 550 breaches affecting 500 or more individuals in the past 24 months.[115] CPL, alone, has the fourth-highest number of patients

[113] FTC, *Privacy and Security Enforcement*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited March 21, 2022).

[114] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Sept. 27, 2019) ("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.").

[115] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,* U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Oct. 9, 2019).

damaged by this Data Breach. As described above, Defendants' other entities make up hundreds of thousands more.[116]

220. As early as 2014, the FBI alerted the healthcare industry that they were an increasingly preferred target of threat actors, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (PII)" so that these companies could take the necessary precautions to thwart such attacks.[117]

221. The co-founder of Lastline, a network security provider, said that "Hackers target financial companies, like this billing collection company, as they often store sensitive financial information that can be turned into immediate gains."[118]

222. 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.[119] With this Data Breach, 2019 has seen the exposure of three times the number of records compromised in 2018.[120]

---

116 *Id.*

117 Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited Sept. 27, 2019).

118 Christopher Rowland, *Quest Diagnostics discloses breach of patient records*, WASH. POST, June 3, 2019, https://www.washingtonpost.com/business/economy/quest-diagnostics-discloses-breach-of-patient-records/2019/06/03/aa37b556-860a-11e9-a870-b9c411dc4312_story.html?utm_term=.78dd30c03a88 (last visited Sept. 27, 2019).

119 *2018 End-of-Year Data Breach Report*, Identity Theft Resource Center, https://www.idtheftcenter.org/2018-data-breaches (last visited Apr. 21, 2019).

120 *Healthcare Data Breach Statistics* (August 2019), HIPPAA Journal, https://www.hipaajournal.com/august-2019-healthcare-data-breach-report (last visited Sept. 27, 2019).

223. Other experts have stated that the Data Breach is at "the intersection of three of the types of data that hackers most desire: personal identifying information that can be used for identity fraud, information about medical conditions, and financial account information."[121]

224. This same article has asked: "why did a collections agency have all of this information in the first place?"[122] It also questioned why medical information and Social Security Numbers needed to be provided to debt collectors.[123]

225. Further, Cathy Allen, CEO of Shared Assessments, a cyber-risk management group, stated that "just the types of test proscribed might indicate a type of illness that you would not want employers or insurance companies to have. Thieves often steal and resell insurance data on the internet . . . having other information makes the data more valuable and the price higher."[124]

226. Personal Information is a valuable commodity to identity thieves. Compromised Personal Information is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers,

---

121 Scott Ikeda, *Third Party Data Breach Hits Quest Diagnostics with 12 Million Confidential Patient Records Exposed*, CPO Magazine, June 11, 2019, https://www.cpomagazine.com/cyber-security/third-party-data-breach-hits-quest-diagnostics-with-12-million-confidential-patient-records-exposed/ (last visited Oct. 7, 2019).

122 *Id.*

123 *Id.*

124 *Id.*

social security numbers and other Personal Information directly on various dark web[125] sites making the information publicly available.[126]

227. Healthcare data is especially valuable on the black market. According to one report, records of healthcare data may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[127]

228. According to a *Reuters* investigation that included interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts, medical data for sale on underground markets "includes names, birth dates, policy numbers, diagnosis codes and billing information" which fraudsters commonly use "to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers."[128]

229. According to Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black, "Health information is a treasure trove for criminals [because] by compromising it, by stealing it, by having it sold, you have seven to 10 personal identifying characteristics of an

---

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

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

[127] *Hackers, Breaches, and the Value of Healthcare Data* (Feb, 2, 2022), https://www.securelink.com/blog/healthcare-data-new-prize-hackers/ (last visited Mar. 21, 2022).

[128] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (last visited Jan. 7, 2022).

individual."[129] For this reason, a patient's full medical records can sell for up to $1,000 on the dark web, while credit card numbers and Social Security numbers may cost $5 or less.[130]

230. As noted by Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies: "The reason for this price discrepancy—like any other good or service—is perceived value. While a credit card number is easily canceled, medical records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information. Once records are stolen, cybercriminals often tap into members of a criminal network on the dark web experienced in drug trafficking and money laundering who are eager to buy medical records to support their criminal activities, such as illegally obtaining prescription medications, filing bogus medical claims or simply stealing the patient's identity to open credit cards and fraudulent loans."[131]

231. Defendants were well aware that their own data and the data they shared with AMCA contained a treasure trove of material for threat actors as it has been targeted in the past. In September 2017, a CPL subsidiary's employee's laptop was stolen, which potentially impacted 500 individuals, putting their names, addresses, social security numbers, drivers' license numbers,

---

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

[130] *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/ (last visited March 21, 2022).

[131] *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web* (Jan. 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last visited March 21, 2022).

medical record information numbers, and/or medical treatment information at risk.[132] Data breaches in the medical community are common, should be anticipated,[133] and should be guarded against. Defendants are not strangers to cyberattacks or theft of PII and PHI.

VIII. Defendants have harmed Plaintiffs and Class Members by allowing anyone to access their information.

232. Defendants caused harm to Plaintiffs and Class Members by sharing their Personal Information with AMCA without properly monitoring a business associate, and AMCA failed to prevent attackers from accessing and stealing Plaintiffs' and Class Members' Personal Information in the Data Breach.

233. Given the sensitive nature of the Personal Information stolen in the Data Breach—including names, mailing addresses, phone numbers, dates of birth, Social Security numbers, information related to Plaintiffs' and Class Members' medical providers and services (such as dates of service, medical condition or disease, treatment, and referring doctor) and other personal information (such as credit and debit card numbers, bank account information, insurance, insurance subscriber identification number), threat actors have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future.

234. In fact, numerous victims of the Data Breach have likely already experienced harms as the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, medical and healthcare fraud, and

---

[132] Elizabeth Snell, SAMBA Mailing Error Creates Data Security Concern for 13.9K, Health IT Security (Mar. 29, 2018), https://healthitsecurity.com/news/samba-mailing-error-creates-data-security-concern-for-13.9k.

[133] *See, e.g.,* HIPAA Breach News, https://hipaaclicks.com/category/hipaa-breach-news/ (last accessed Nov. 14, 2019).

unauthorized access to their bank accounts. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

235. The PII and PHI exposed in the Data Breach is highly coveted and valuable on underground or black markets and information tied to this Data Breach has already been offered for sale. For example, identity thieves can use the stolen information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest. Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail, extortion, and other negative effects.

236. While federal law generally limits an individual's liability for fraudulent credit card charges to $50, there are no such protections for a stolen medical identity. According to a 2015 survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft spent an average of $13,500 in out-of-pocket costs to resolve the crime.[134] Frequently, this information was used to obtain medical services or treatments (59%), obtain prescription drugs

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

(56%), or receive Medicare and Medicaid benefits (52%). Only 14% of respondents said that the identity thieves used the information to obtain fraudulent credit accounts, indicating that medical information is a much more profitable market.[135]

237. According to the Ponemon study, "[t]hose who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate."[136]

238. Additionally, the study found that medical identity theft can have a negative impact on reputation as 45% of respondents said that medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions, with 19% responding that they missed out on employment opportunities as a result.[137]

239. Exacerbating the problem, victims of medical identity theft oftentimes struggle to resolve the issue because HIPAA regulations require the victim to be personally involved in the resolution of the crime.[138] In some cases, victims may not even be able to access medical records using their personal information because they include a false name or data points taken from another person's records. Consequently, only 10% of medical identity theft victims responded that they "achiev[ed] a completely satisfactory conclusion of the incident."[139]

---

[135] *Id*. at 9.

[136] *Id*. at 2.

[137] *Id*. at 14.

[138] *Id*. at 1.

[139] *Id*.

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

- Receive a bill for medical service that they did not receive;
- Get contacted by a debt collector about medical debt they do not owe;
- See medical collection notices on their credit report that they do not recognize;
- Find erroneous listings of office visits or treatments on their explanation of benefits (EOB);
- Receive information from their health plan that they have reached their limit on benefits; or
- Be denied insurance because their medical records show a condition they do not have.[140]

241. Other types of medical fraud include "leveraging details specific to a disease or terminal illness, and long-term identity theft."[141] According to Tom Kellermann, "Traditional criminals understand the power of coercion and extortion. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[142] Long-term identity theft

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

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

[142] *Id.*

occurs when fraudsters combine a victim's data points, including publicly-available information or data points exposed in other data breaches, to create new identities, open false lines of credit, or commit tax fraud that can take years to remedy.

242. Medical data is particularly valuable to threat actors. In June 2016, a hacker reportedly was offering to sell hacked medical records of nearly 700,000 patients for hundreds of thousands of dollars on a "deep web marketplace."[143] Later, the same hacker revealed that he had a database of 9.3 million records from a U.S. insurer that were for sale. [144]

243. In a data breach implicating a medical provider or medical information, consumers face the additional risk of their Health Savings Accounts ("HSAs") being compromised. HSAs are often tied to specialized debit cards used to make medical-based payments. However, they can also be used for regular purchases (albeit incurring a severe tax penalty). Such information is an "easy target" for criminal actors.[145]

244. Fraudulent charges have already been linked to Defendants' billing collector's data handling. Another lab impacted by the Data Breach publicly revealed the exposure of patients' Personal Information only after "a disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges."[146]

---

143 Healthcare under Attack: What Happens to Stolen Medical Records?, June 30, 2016, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/healthcare-under-attack-stolen-medical-records (last visited Sept. 27, 2019).

144 Lording it over the healthcare sector: health insurer database with 9.3M entries up for sale, https://www.databreaches.net/lording-it-over-the-healthcare-sector-health-insurer-database-with-9-3m-entries-up-for-sale/, (last visited Sept. 27, 2019).

145 *Id.*

146 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. June 17, 2019), ECF No. 2 at 5-6.

245. In addition, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[147] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

246. As explained further by the FTC, medical identity theft can have other serious consequences:

> Medical ID thieves may use your identity to get treatment—even surgery—or to bilk insurers by making fake claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits, and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[148]

247. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[149]

---

147 *The Aftermath 2017*, Identity Theft Resource Center, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Aug. 9, 2019).

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

149 *See Study: Medical identity theft is costly for victims,* CNET (Mar. 3, 2010), *available at* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Oct. 11, 2019).

248. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their Personal Information;

b. identity theft and fraud resulting from the theft of their Personal Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

h. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

249. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[150]

250. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the United States Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[151]

251. Plaintiffs and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a

---

150 E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Aug. 9, 2019).

151 U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (2007), *available at* http://www.gao.gov/new.items/d07737.pdf.

provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[152]

252. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, Defendants would have no reason to tout their data security efforts to their actual and potential customers.

253. Consequently, had consumers known the truth about Defendants' data security practices—that they did not adequately protect and store their Personal Information—they would not have entrusted their Personal Information to Defendants.

254. Reactions to the Data Breach reflect the severity and breadth of the adverse impact on the American public.

255. The Attorney General of Maryland issued a "Consumer Alert" on June 12, 2019, stating, "Massive data breaches like the one experienced by the AMCA are extremely alarming, especially considering the likelihood that personal, financial, and medical information may now be in the hands of thieves and scammers, . . . I strongly urge consumers to take steps to ensure that their information and personal identity is protected."[153]

256. Connecticut Attorney General William Tong, announcing that Illinois and Connecticut's Attorneys General have opened an investigation into the Data Breach, stated:

> The last thing patients should have to worry about is whether their personal information has been compromised by the entities responsible for protecting it. I am committed to ensuring that impacted patients receive timely notification and

---

[152] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited Aug. 9, 2019).

[153] Brian E. Frosh, Attorney General, Maryland, Consumer Alert (June 12, 2019), http://www.marylandattorneygeneral.gov/press/2019/061219.pdf.

> that the companies involved take precautions to protect consumers' sensitive health and financial information in the future.[154]

257. Other State Attorneys General, including the Attorneys General of Michigan, Minnesota, and North Carolina, have also launched investigations into the Data Breach.[155]

CLASS ACTION ALLEGATIONS

258. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following class (the "Class"):

> All natural persons who obtained services from Clinical Pathology Laboratories, American Esoteric Laboratories, CBLPath, Inc., Sunrise Medical Laboratories, Inc., Austin Pathology Associates, Laboratory Medicine Consultants, Ltd., South Texas Dermatology Lab, PLLC, Pathology Solutions, LLC, Seacoast Pathology, Inc., Arizona Dermatopathology, Western Pathology Consultants, Ltd., and Laboratory of Dermatology ADX, LLC who were residing in the United States whose Personal Information was compromised in the Data Breach.

259. The Class asserts claims against Defendants for negligence (Count 1), negligence *per se* (Count 2), breach of confidence (Count 3), invasion of privacy – intrusion upon seclusion (Count 4), and unjust enrichment (Count 5).

260. Excluded from the Class are the Defendants, any entity in which they have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

---

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

155 *AMCA Data Breach Tally Passes 20 Million as BioReference Laboratories Added to List of Impacted Entities*, HIPPA Journal, https://www.hipaajournal.com/amca-data-breach-tally-passes-20-million-as-bioreference-laboratories-added-to-list-of-impacted-entities/ (last visited Oct. 9, 2019).

261. **Numerosity: Federal Rule of Civil Procedure 23(a)(1)**. The members of the Class are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, the individuals impacted by the AMCA Data Breach number in the millions—as stated in paragraph 174, above. Those individuals' names and addresses are available from Defendants' records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

262. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

a. Whether Defendants had a duty to protect Personal Information;

b. Whether Defendants failed to take reasonable and prudent security measures;

c. Whether Defendants knew or should have known of the susceptibility of AMCA's systems to a data breach;

d. Whether Defendants were negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Defendants' security measures to protect their systems were reasonable in light known legal requirements;

f. Whether Defendants were negligent in failing to adequately monitor and audit the data security systems of their vendors and business associates;

g. Whether Defendants' efforts (or lack thereof) to ensure the security of patients' Personal Information provided to business associates were reasonable in light of known legal requirements;

h. Whether Defendants' conduct constituted unfair or deceptive trade practices;

i. Which security procedures and notification procedures Defendants should be required to implement;

j. Whether Defendants have a contractual obligation to use reasonable security measures;

k. Whether Defendants have complied with any contractual obligation to use reasonable security measures;

l. What security measures, if any, must be implemented by Defendants to comply with their contractual obligations;

m. Whether Defendants violated state consumer protection and state medical information privacy laws in connection with the actions described herein;

n. Whether Defendants failed to notify Plaintiffs and Class Members as soon as practicable and without delay after the data breach was discovered;

o. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of AMCA's systems and/or the loss of the Personal Information of Plaintiffs and Class Members;

p. Whether Plaintiffs and Class Members were injured and suffered damages or other losses because of Defendants' failure to reasonably protect their Personal Information; and,

q. Whether Plaintiffs and Class Members are entitled to damages, declaratory relief, or injunctive relief.

263. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class Members. Plaintiffs' Personal Information was in Defendants' possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class Members and Plaintiffs seek relief consistent with the relief of the Class.

264. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Defendants to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

265. **Predominance & Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to

individually litigate their claims against Defendant, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

266. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for Defendants or would be dispositive of the interests of members of the proposed Class.

267. **Ascertainability.** The Class are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the class. The Class consist of individuals who received services from Defendants and whose accounts were placed into collections with AMCA by Defendant. Class Membership can be determined using Defendants' and AMCA's records in their databases.

268. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

269. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Defendants failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiffs and the Class Members;

c. Whether Defendants failed to adequately monitor and audit the data security systems of their vendors and business associates;

d. Whether adherence to HIPAA regulations, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach;

e. Whether Defendants were unfairly and unjustly enriched as a result of their improper conduct, such that it would be inequitable for Defendants to retain the benefits conferred upon them by Plaintiffs and the Class Members.

COUNT 1

NEGLIGENCE

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

271. Plaintiffs bring this claim against all Defendants.

272. Defendants required Plaintiffs and Class Members to submit Personal Information to obtain diagnostic and medical services, which Defendants provided to AMCA for billing purposes. Defendants collected and stored the Personal Information for commercial gain.

273. Defendants knew or should have known that AMCA's web payments page was vulnerable to unauthorized access by third parties.

274. Defendants had non-delegable duties to ensure that contractual partners with whom they shared patient information maintained adequate and commercially-reasonable data security practices to ensure the protection of patients' Personal Information.

275. Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' Personal Information within their control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

276. Defendants owed a duty of care to Plaintiffs and members of the Class to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the Personal Information.

277. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and the Plaintiffs and Class Members. The special relationship arose because Plaintiffs and Class Members entrusted Defendants with their confidential data as part of the health treatment process. Only Defendants were in a position to ensure that their contractual partners had sufficient safeguards to protect against the harm to Plaintiffs and Class Members that would result from a data breach.

278. Defendants' duty to use reasonable care in protecting Personal Information arose as a result of the common law and the statutes and regulations, as well as their own promises

regarding privacy and data security to their patients. This duty exists because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of Plaintiffs and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they would be harmed in the future if Defendants did not protect Plaintiffs' and Class Members' information from threat actors.

279. Defendants' duties also arose under HIPPA regulations, which, as described above, applied to Defendants and establish national standards for the protection of patient information, including protected health information, which required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The duty also arose under HIPAA's Privacy Rule requirement that Defendants obtain satisfactory assurances from their business associate AMCA that AMCA would appropriately safeguard the protected health information they receive or creates on behalf of Defendants. 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

280. Defendants' duties also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits their "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of Defendants' duty. In addition, several individual states have enacted statutes based upon the FTC Act that also created a duty.

281. Defendants knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of their vendors' and business associates' systems, and the importance of adequate security.

282. Defendants breached their common law, statutory, and other duties—and thus were negligent—by failing to use reasonable measures to protect patients' Personal Information, and by failing to provide timely and adequately detailed notice of the Data Breach.

283. Defendants breached their duties to Plaintiffs and Class Members in numerous ways, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs' and Class Members' Personal Information;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

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

d. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

e. Failing to adequately monitor, evaluate, and ensure the security of AMCA's network and systems;

f. Failing to recognize in a timely manner that Plaintiffs' and other Class Members' Personal Information had been compromised; and

g. Failing to timely and adequately disclose that Plaintiffs' and Class Members' Personal Information had been improperly acquired or accessed.

284. Plaintiffs' and Class Members' Personal Information would not have been compromised but for Defendants' wrongful and negligent breach of their duties.

285. Defendants' failure to take proper security measures to protect sensitive Personal Information of Plaintiffs and Class Members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Personal Information of Plaintiffs and Class Members.

286. It was also foreseeable that Defendants' failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and other Class Members.

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

288. As a direct and proximate cause of Defendants' conduct, Plaintiffs and the Class suffered damages and will suffer damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the Personal Information of Plaintiff and Class Members; damages arising from identity theft or fraud; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take years to discover and detect; and loss of the value of their privacy and confidentiality of the stolen confidential data, including health data.

289.

COUNT 2

NEGLIGENCE PER SE

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

291. Plaintiffs bring this claim against all Defendants.

292. Defendants are entities covered by HIPAA (45 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

293. HIPAA requires Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). HIPAA also requires Defendants to obtain satisfactory assurances that their business associates would appropriately safeguard the protected health information they receive or creates on behalf of the Defendant. 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA. AMCA constitutes a "business associate" within the meaning of HIPAA.

294. HIPAA further requires Defendants to disclose the unauthorized access and theft of the Personal Information to Plaintiffs and the Class Members "without unreasonable delay" so that Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information. *See* 45 C.F.R. §§ 164.404, 406, 410.

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

296. Defendants' violations of HIPAA constitute negligence per se.

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

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

299. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

300. The FTC publications and orders described above also form part of the basis of Defendants' duties in this regard.

301. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Personal Information they obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as Defendants, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

302. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

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

304. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

305. As a direct and proximate result of Defendants' negligence per se under HIPAA and the FTC Act, Plaintiffs and the Class have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT 3

BREACH OF CONFIDENCE

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

307. Plaintiffs bring this claim against all Defendants.

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

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

310. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' Personal Information in violation of this understanding. The unauthorized disclosure occurred because Defendants failed to implement and maintain reasonable safeguards

to protect the Personal Information in their possession and failed to comply with industry-standard data security practices.

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

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

COUNT 4

INVASION OF PRIVACY – INTRUSION UPON SECLUSION

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

314. Plaintiffs bring this claim against all Defendants.

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

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

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

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

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

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

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

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

COUNT 5

UNJUST ENRICHMENT

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

320. For years and continuing to today, Defendants' business model has depended upon patients entrusting them with their Personal Information. Trust and confidence are critical and central to both the services provided by Defendants to patients and the billing and collection for such services. Unbeknownst to Plaintiffs and Class Members, however, Defendants failed to ensure their vendors and business associates reasonably or adequately secured, safeguarded, and otherwise protected Plaintiffs' and Class Members' Personal Information. Defendants' deficiencies described herein were contrary to their security messaging.

321. Plaintiffs and Class Members engaged Quest for services and provided Defendants with, and allowed Defendants to collect, their Personal Information on the mistaken belief that

Defendants complied with their duty to safeguard and protect patients' Personal Information. Putting their short-term profit ahead of safeguarding Personal Information, and unbeknownst to Plaintiffs and Class Members, Defendants knowingly sacrificed security in favor of collecting moneys Defendants believed were owed. Defendants knew that the manner in which they maintained and transmitted patients' Personal Information violated their fundamental duties to Plaintiffs and Class Members by disregarding industry-standard security protocols to ensure confidential information was securely transmitted and stored.

322. Defendants had within their exclusive knowledge at all times relevant that their vendors and business associates failed to implement adequate security measures to keep patients' Personal Information secure. This information was not available to Plaintiffs, Class Members, or the public at large.

323. Defendants also knew that Plaintiffs and Class Members expected that their information would be kept secure against known security risks and that the security protocols of any vendors or business associates used by Defendants would be thoroughly vetted before they received patients' Personal Information.

324. Plaintiffs and Class Members did not expect that Defendants would engage a billing collection agency, AMCA, that employed substantially deficient security protocols and would store highly sensitive PHI that was irrelevant to collecting payments.

325. Had Plaintiffs and Class Members known about Defendants' practice of sharing their Personal Information with vendors and business associates who were unequipped to protect it—and insecurely transmitting sensitive PHI that had no bearing on collecting payments—, Plaintiffs and Class Members would not have engaged Defendants to perform any services and would never have provided Defendants with their Personal Information.

326. By withholding these material facts, Defendants put their own interests ahead of their patients' interests and benefitted themselves to the detriment of Plaintiffs and Class Members.

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

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

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

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

REQUESTS FOR RELIEF

Plaintiffs, individually and on behalf of members of the Class, as applicable, respectfully request that the Court enter judgment in their favor and against Defendants, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Co-Lead and Co-Liaison Counsel as Class Counsel;

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

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

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of its unlawful acts, omissions, and practices;

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

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

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

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

9. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.
Interim Lead Counsel for Plaintiffs

By: /s/ James E. Cecchi
JAMES E. CECCHI

Dated: March 31, 2022

Joseph J. DePalma
Bruce D. Greenberg
LITE DEPALMA GREENBERG & AFANADOR LLC
570 Broad Street, Suite 1201
Newark, New Jersey 07102
(973) 623-3000

Joseph P. Guglielmo
SCOTT+SCOTT ATTORNEYS AT LAW, LLP
The Helmsley Building
230 Park Ave, 17th Floor
New York, New York 10169
(212) 223-6444

Amy E. Keller
Adam J. Levitt
DICELLO LEVITT GUTZLER LLC
10 North Dearborn Street, 11th Floor
Chicago, Illinois 60602
(312) 214-7900

Other Labs Track Co-Lead Counsel

James Pizzirusso
Katie R. Beran
HAUSFELD LLP
1700 K Street, NW, Suite 650
Washington, DC 20006
(202) 540-7200

Laurence D. King
Mario M. Choi
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
(415) 772-4700

Other Labs Track Steering Committee