Exhibit C1

IN THE UNITED STATES DISTRCT COURT
FOR THE DISTRICT OF KANSAS

DAVID FINCH, on behalf of himself and all others similarly situated, Plaintiff, vs. LABORATORY CORPORATION OF AMERICA HOLDINGS d/b/a LABCORP, and AMERICAN MEDICAL COLLECTION AGENCY, INC. Defendants.	Case No. 2:19-cv-2307 CLASS ACTION JURY TRIAL DEMANDED

COMPLAINT

Plaintiff David Finch, on behalf of himself and all others similarly situated, by and through his undersigned attorneys of record, for his Complaint against Defendants Laboratory Corporation of America Holdings d/b/a LabCorp ("LabCorp") and American Medical Collection Agency, Inc. ("AMCA") (collectively, "Defendants"), and states to the Court as follows:

1. This is a data breach class action on behalf of 7.7 million patients whose sensitive personal information was accessed by computer hackers in a cyber-attack (the "Data Breach"). Information compromised in the Data Breach includes Social Security numbers, financial information (*e.g.*, credit card numbers and bank account information), medical information, other protected health information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personal information (collectively, "Sensitive Information").

2. Plaintiff brings this class action lawsuit on behalf of a Nationwide class and a Kansas Statewide sub-class to address Defendants' inadequate safeguarding of class members' Sensitive Information.

3. Armed with the Sensitive Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in class members' names, taking out loans in class members' names, using class members' names to obtain medical services, using class members' health information to target other phishing and hacking intrusions based on their individual health needs, using class members' information to obtain government benefits, filing fraudulent tax returns using class members' information, obtaining driver's licenses in class members' names but with another person's photograph, and giving false information to police during an arrest.

4. As a result of the Data Breach, Plaintiff and class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and class members must now and in the future closely monitor their financial accounts to guard against identity theft.

5. Plaintiff and class members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

6. Plaintiff seeks to remedy these harms on behalf of himself and all similarly-situated individuals whose Sensitive Information was accessed during the Data Breach.

7. Plaintiff seeks remedies including but not limited to compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to

Defendants' data security systems, future annual audits, and free credit monitoring services funded by Defendants.

PARTIES

8. Plaintiff David Finch is an individual residing in Kansas. He has been a patient of LabCorp when LabCorp collected and received Plaintiff's Sensitive Information in Kansas which LabCorp maintained in its database. His Sensitive Information, on information and belief, was compromised in the data breach.

9. At this time of this filing, Plaintiff David Finch was a debtor in a Chapter 13 Bankruptcy case pending in the District of Kansas, case number 19-20458 and only recently became aware of the Data Breach. Plaintiff will amend his bankruptcy schedules to disclose this recently discovered claim to the Bankruptcy Court. Plaintiff David Finch's Chapter 13 Plan was confirmed on May 15, 2019.

10. Defendant Laboratory Corporation of America Holdings d/b/a LabCorp is incorporated in Delaware. Its principal place of business is in Burlington, North Carolina.

11. Defendant American Medical Collection Agency, Inc. ("AMCA") is incorporated in Minnesota. Its principal place of business is in Elmsford, New York.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5 million exclusive of interest and costs, and many members of the class are citizens of states different from Defendants.

13. This Court has personal jurisdiction over Defendants because Defendants conduct business in and throughout Kansas, Plaintiff and the class members provided

LabCorp with their Sensitive Information in Kansas and that Sensitive Information was used by Defendants to attempt to collect alleged medical bills inside the State of Kansas.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to Plaintiff's claims occurred in this District. Venue is also proper pursuant to 28 U.S.C. § 1391(b)(1) because all defendants are residents for venue purposes because they regularly transact business here. Further, venue is proper under 28 U.S.C. § 1391(b)(3) because all Defendants are subject to personal jurisdiction in this District.

FACTUAL ALLEGATIONS

15. LabCorp a leading provider of medical diagnostic testing services. It performs medical tests that aid in the diagnosis or detection of diseases, and that measure the progress of or recovery from a disease.

16. LabCorp's invoices cover laboratory testing fees only and are separate from any bill received by a patient's physician. Patients can be charged by either directly going to a LabCorp facility or if their physician has sent their specimen to a LabCorp laboratory.

17. When certain LabCorp customers do not pay their invoices within the requested time period, LabCorp will reach out to a collection agency like AMCA.

18. Upon information and belief, LabCorp would provide AMCA with LabCorp customers' Sensitive Information, which AMCA subsequently housed in its own system, in order to facilitate collections. This information included first and last name, date of birth, address, phone, date of service, provider, and balance information.

19. On June 4, 2019, LabCorp publicly announced the following, in relevant part, in a Form 8-K filed with the Securities and Exchange Commission:

According to AMCA, this activity occurred between August 1, 2018, and March 30, 2019. AMCA is an external collection agency used by LabCorp and other healthcare companies. LabCorp has referred approximately 7.7 million consumers to AMCA whose data was stored in the affected AMCA system. AMCA's affected system included information provided by LabCorp. That information could include first and last name, date of birth, address, phone, date of service, provider, and balance information. AMCA's affected system also included credit card or bank account information that was provided by the consumer to AMCA (for those who sought to pay their balance). LabCorp provided no ordered test, laboratory results, or diagnostic information to AMCA. AMCA has advised LabCorp that Social Security Numbers and insurance identification information are not stored or maintained for LabCorp consumers.

AMCA has informed LabCorp that it is in the process of sending notices to approximately 200,000 LabCorp consumers whose credit card or bank account information may have been accessed. AMCA has not yet provided LabCorp a list of the affected LabCorp consumers or more specific information about them.[1]

20. Defendant AMCA failed to properly safeguard class members' Sensitive Information, allowing hackers to access their Sensitive Information for eight months. AMCA also failed to properly monitor its systems. Had it properly monitored its systems, it would have discovered the intrusion much sooner than eight months after the breach began.

---

[1] http://secfilings.nasdaq.com/filingFrameset.asp?FilingID=13474097&RcvdDate=6/4/2019&CoName=LABORATORY%20CORP%20OF%20AMERICA%20HOLDINGS&FormType=8-K&View=html (last accessed June 13, 2019).

21. Defendant LabCorp failed to properly monitor its vendors to ensure that proper data security safeguards were being implemented by those vendors throughout the breach period.

22. Defendants had obligations created by HIPAA, industry standards, common law, and representations made to class members, to keep class members' Sensitive Information confidential and to protect it from unauthorized access and disclosure.

23. Plaintiff and class members provided their Sensitive Information to LabCorp with the reasonable expectation and mutual understanding that LabCorp and any business partners to which LabCorp disclosed the Sensitive Information would comply with their obligations to keep such information confidential and secure from unauthorized access.

24. Indeed, LabCorp promised patients that it will keep their Sensitive Information confidential, stating in its Notice of Privacy Practices that it is "committed to the protection of your PHI and will make reasonable efforts to ensure the confidentiality of your PHI, as required by statute and regulation."[2] LabCorp's Notice of Privacy Practices also acknowledged that LabCorp is subject to HIPAA.[3]

25. LabCorp further stated in its Notice of Privacy Practices that its vendors maintain adequate data security over patient data, stating:

> LabCorp may disclose PHI to its business associates to perform certain business functions or provide certain business services to LabCorp. For example, we may use

[2] *See* https://www.labcorp.com/hipaa-privacy/hipaa-notice-privacy-practices# (last accessed June 13, 2019).

[3] *Id.*

another company to perform billing services on our behalf. All of our business associates are required to maintain the privacy and confidentiality of your PHI.[4]

26. Defendants' data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach. The increase in data breaches, and attendant risk of future breaches, was widely known to the public and to anyone in Defendants' industries, including Defendants.

A. Defendants' Data Security Failures and HIPAA Violations

27. Defendants' data security failures demonstrate that they failed to honor their duties and promises by not:

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

b. Adequately protecting patients' Sensitive Information;

c. Properly monitoring their own data security systems for existing intrusions;

d. Ensuring that their vendors employed reasonable data security procedures;

e. Ensuring the confidentiality and integrity of electronic protected health information ("PHI") they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Implementing technical policies and procedures for electronic information systems that maintain electronic PHI 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);

---

[4] *Id.*

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

h. Implementing 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);

i. Protecting against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

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

k. Ensuring compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4); and/or

l. Training all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b).

B. Damages to Class Members

28. Plaintiff and class members have been damaged by the compromise of their Sensitive Information in the Data Breach.

29. Plaintiff and class members face substantial risk of out of pocket fraud losses such as loans opened in their names, medical services building their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

30. Plaintiff and class members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PHI as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and class members.

31. Plaintiff and class members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

32. Plaintiff and class members suffered a "loss of value" of their Sensitive Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of quote loss of value" damages in data breach cases.

33. Class members who paid LabCorp for its services were also damaged via "benefit of the bargain" damages. Such class members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price class members paid to LabCorp was intended to be used by LabCorp to fund adequate data security and monitor its vendors' compliance with data security obligations. LabCorp did not properly monitor its vendors' compliance with data security obligations. Thus, the class members did not get what they paid for.

34. Plaintiff and class members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

35. The U.S. Government Accountability Office noted in a report on data breaches (the "GAO Report") that identity thieves often use identifying data such as Social Security numbers to open financial accounts, receive government benefits, and incur charges and

credit in a person's name.[5] As the GAO Report states, this type of identity theft is particularly harmful because it often takes time for the victim to become aware of the theft, and the theft can adversely impact the victim for years.

36. In addition, the GAO Report states that victims of identity theft may face "substantial costs and inconveniences repairing damage to their credit records."[6] identity theft victims are frequently required to spend many hours as well as money repairing the impact to their credit.

37. There may be a substantial time lag — measured in years — between when sensitive information is stolen and when it is used. According to the GAO Report: "[O]nce stolen data have been sold or posted to 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."[7] thus, plaintiff in class members must vigilantly monitor their financial and medical accounts for many years to come.

38. With access to the type of information that was accessed in the Data Breach, criminals can use the information gained to gather additional information about Plaintiff and class members, open accounts in victims' names; receive medical service in the victims' name; obtain a driver's license or official identification card in the victim's name but with the thief's photo; use the victim's name and Social Security number to obtain government benefits; file a fraudulent tax return using the victim's information; and give the victim's

---

[5] *See* https://www.gao.gov/new.items/d07737.pdf (last accessed June 12, 2019).

[6] *Id.*

[7] *Id.*

personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[8]

39. The Sensitive Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often sell it on the cyber "black-market" or "dark web" indefinitely. Cyber criminals routinely post stolen Social Security numbers, financial information, medical information, and other sensitive personal information on anonymous websites, making the information widely to a criminal underworld. There is an active and robust market for this information.

40. Medical information is especially valuable to identity thieves. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. Defendants knew or should have known this and strengthened their data systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

CLASS ACTION ALLEGATIONS

41. Plaintiff brings this case as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of a Nationwide Class defined as follows:

> All persons in the United States who utilized LabCorp's services and whose Sensitive Information was maintained on AMCA's system that was compromised in the data breach announced by LabCorp on June 3, 2019.

---

[8] *See* Federal Trade Commission, Warning Signs of Identity Theft, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed June 12, 2019).

and a Statewide Sub-Class defined as follows:

> All persons in the State of Kansas who utilized LabCorp's services and whose Sensitive Information was maintained on AMCA's system that was compromised in the data breach announced by LabCorp on June 3, 2019.

42. Excluded from the above Classes are Defendants' executive officers, and the judge to whom this case is assigned.

43. **Numerosity**. The Classes are each so numerous that joinder of all members is impracticable. The Class consists of hundreds, if not thousands or more individuals, on information and belief.

44. **Commonality**. There are many questions of law and/or fact common to Plaintiff and the class. Common questions include, but are not limited to:

a. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

b. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendants owed a duty to class members to safeguard their Sensitive Information;

d. Whether Defendants breached their duty to class members to safeguard their Sensitive Information;

e. Whether computer hackers obtained class members' Sensitive Information in the Data Breach;

f. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

g. Whether Plaintiff and class members suffered legally cognizable damages as a result of Defendant's misconduct; and

h. Whether Plaintiff and class members are entitled to injunctive relief.

45. **Typicality**. Plaintiff's claims are typical of the claims of class members in that Plaintiff, like all class members, had his personal information compromised in the Data Breach.

46. **Adequacy of Representation**. Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has retained competent and capable counsel with significant experience in complex class action litigation. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Classes. Plaintiff's counsel has the financial and personnel resources to do so. Neither Plaintiff nor his counsel have interests that are contrary to, or that conflict with, those of the Classes.

47. **Predominance**. Defendants have engaged in a common course of conduct toward Plaintiff and class members. The common issues arising from Defendants' conduct affecting class members predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

48. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would likely find that the cost of litigating their individual claim

is prohibitively high and would Therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

49. Defendants have acted on grounds that apply generally to the Classes as a whole, so that injunctive relief is appropriate on a class-wide basis under Fed. R. Civ. P. 23(b)(2).

COUNT I
NEGLIGENCE

50. Plaintiff re-alleges and incorporates by reference all preceding allegations.

51. LabCorp required Plaintiff and class members to submit non-public personal information in order to obtain medical services, which it forwarded to AMCA for billing purposes.

52. By collecting and storing this data, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard class members' Sensitive Information, to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

53. Defendants owed a duty of care to Plaintiff and class members to provide data security consistent with industry standards and other requirements discussed herein, and

to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Sensitive Information.

54. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between LabCorp and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to class members from a data breach.

55. Defendants' duty to use reasonable security measures under HIPAA 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). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

57. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Sensitive Information.

58. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect class members' Sensitive Information, and by failing to

provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard class members' Sensitive Information;

b. Failing to adequately monitor the security of AMCA's networks and systems;

c. Failure by LabCorp to periodically ensure that its vendors, including AMCA, had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to class members' Sensitive Information;

e. Failing to detect in a timely manner that class members' Sensitive Information had been compromised; and

f. Failing to timely notify class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

59. It was foreseeable that Defendants' failure to use reasonable measures to protect class members' Sensitive Information would result in injury to class members. Further, the breach of security was reasonably foreseeable given the known high frequency of data breaches in the medical industry.

60. It was therefore foreseeable that the failure to adequately safeguard class members' Sensitive Information would result in one or more types of injuries to class members.

61. Plaintiff and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

62. Plaintiff and class members are also entitled to injunctive relief requiring Defendants to, e.g.,: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all class members.

COUNT II
BREACH OF IMPLIED CONTRACT

63. Plaintiff re-alleges and incorporates by reference all preceding allegations.

64. When Plaintiff and class members provided their Sensitive Information to Defendants in exchange for Defendants' services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

65. Defendants solicited and invited class members to provide their Sensitive Information as part of Defendants' regular business practices. Plaintiff and class members accepted Defendants' offers and provided their Sensitive Information to Defendants.

66. In entering into such implied contracts, Plaintiff and class members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

67. Class members were aware of, or reasonably anticipated that, LabCorp would forward certain Sensitive Information to vendors, as disclosed in LabCorp's Notice of Privacy Practices.

68. Class members who paid money to LabCorp reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

69. Plaintiff and class members would not have entrusted their Sensitive Information to Defendants in the absence of the implied contract between them and Defendants to keep the information reasonably secure. Plaintiff and class members would not have entrusted their Sensitive Information to LabCorp in the absence of LabCorp's implied promise to monitor its vendors to ensure that they adopted reasonable data security measures.

70. Plaintiff and class members fully and adequately performed their obligations under the implied contracts with Defendants.

71. Defendants breached their implied contracts class members by failing to safeguard and protect their Sensitive Information. LabCorp breached its implied contract with class members by failing to properly monitor the data security practices of its vendors, AMCA.

72. As a direct and proximate result of Defendants' breaches of the implied contracts, class members sustained damages as alleged herein.

73. Plaintiff and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

74. Plaintiff and class members are also entitled to injunctive relief requiring Defendants to, e.g.,: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all class members.

COUNT III
KAN. STAT. ANN. § 50-7A02(A), ET SEQ.
(Kansas sub-class only)

75. Plaintiff re-alleges and incorporates by reference all preceding allegations.

76. Defendants are required to accurately notify Plaintiff and Class Members if Defendants become aware of a breach of their data security system (that was reasonably likely to have caused misuse of Plaintiff's and Class Members' Sensitive Information) in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

77. Defendants are businesses that own or license computerized data that includes personal information as defined by Kan. Stat. Ann. § 50-7a02(a).

78. Plaintiff and Class Members' Sensitive Information (e.g., Social Security numbers) includes personal information as covered under Kan. Stat. Ann. § 50-7a02(a).

79. Because Defendants were aware of a breach of their security system (that was reasonably likely to have caused misuse Plaintiff and Class Members' Sensitive Information), Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

80. Thus, by failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Kan. Stat. Ann. § 50-7a02(a).

81. As a direct and proximate result of Defendants' violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Class Members suffered damages, as described above.

82. Plaintiff and Class Members seek relief under Kan. Stat. Ann. § 50-7a02(g), including, but not limited to, broad equitable relief.

COUNT IV
NEGLIGENCE PER SE

83. Plaintiff re-alleges and incorporates by reference all preceding allegations.

84. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Sensitive Information.

85. Pursuant to HIPAA (42 U.S.C. § 1302d, et seq.), Defendants had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Sensitive Information.

86. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendants had a duty to protect the security and confidentiality of Plaintiff's and Class Members' Sensitive Information.

87. Defendants breached their duties to Plaintiff and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d et. seq.), and Gramm- Leach-Bliley Act (15 U.S.C. § 6801) by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Sensitive Information.

88. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

89. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

90. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Sensitive Information.

91. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT V
BREACH OF FIDUCIARY DUTY

92. Plaintiff re-alleges and incorporates by reference all preceding allegations.

93. In light of the special relationship between Defendants and Plaintiff and Class Members, whereby Defendants became guardians of Plaintiff's and Class Members' Sensitive Information, Defendants became fiduciaries created by their undertaking and guardianship of the Sensitive Information, to act primarily for the benefit of their patients, including Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' Sensitive Information; (2) to timely notify Plaintiff and Class Members' of a data breach and disclosure; and (3) maintain complete and accurate records of what and where Defendants' patients' information was and is stored.

94. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their patients' relationship, in particular, to keep secure the Sensitive Information of their patients.

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

96. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Sensitive Information.

97. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

98. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendants created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

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

100. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

101. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

102. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. § 164.306(a)(2).

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

104. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by their workforce in violation of 45 C.F.R. § 164.306(a)(94).

105. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

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

107. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. § 164.530(c).

108. Defendants breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Sensitive Information.

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

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

RELIEF REQUESTED

111. Plaintiff, on behalf of all others similarly situated, requests that the Court enter judgment against Defendants including the following:

a. Determining that this matter may proceed as a class action and certifying the classes asserted herein;

b. Appointing Plaintiff as representative of each of the classes and Plaintiff's counsel as class counsel;

c. An award to Plaintiff and the Class of compensatory and consequential damages;

d. Injunctive relief requiring Defendants to, e.g.,: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all class members;

e. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

f. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

g. Such other or further relief as the Court may allow.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

Dated: June 13, 2019

Respectfully submitted,

LEAR WERTS LLP

Todd C. Werts KS Bar # 20524
Bradford B. Lear, *pro hac vice forthcoming*
2003 West Broadway, Suite 107
Columbia, Missouri 65203
Tel: 573-875-1991
Fax: 573-875-1985
Email: lear@learwerts.com
Email: werts@learwerts.com

CALLAHAN LAW FIRM, LLC
Ryan M. Callahan KS Bar # 25363
222 W. Gregory Blvd., Ste. 210
Kansas City, MO 64114
Tel: 913-601-1620
Email: ryan@callahanlawkc.com

COHEN & MALAD LLP
Lynn Toops, *pro hac vice forthcoming*
One Indiana Square, Suite 1400
Indianapolis, IN 46204
Tel: 317-636-6481
Fax: 317-636-2593
Email: ltoops@cohenandmalad.com

ATTORNEYS FOR PLAINTIFF