UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

DANIEL DURGIN, individually and on behalf of all others similarly situated, Plaintiff, v. TRANSFORMATIVE HEALTHCARE, LLC, and COASTAL MEDICAL TRANSPORTATION SYSTEMS, LLC, Defendants.	)	Case No.: **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Daniel Durgin ("Plaintiff"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Defendants Transformative Healthcare, LLC and Coastal Medical Transportation Systems, LLC (collectively, " Defendants"). Based upon personal knowledge, information, belief, and investigation of counsel, Plaintiff specifically alleges as follows:

NATURE OF THE CASE

1. Plaintiff brings this class action against Defendants for their failure to exercise reasonable care in securing and safeguarding individuals' sensitive personal information, including their sensitive personal health information ("PHI"), on a massive scale.

2. On April 21, 2023, Transformative Healthcare, LLC ("Transformative") first learned that an unauthorized party gained access to archival data from the computer network of defunct emergency services provider Fallon Ambulance Service ("Fallon"), which Coastal

Medical Transportation Systems, LLC ("Coastal") had acquired from Transformative in September 2022.

3. It was not until on or about December 27, 2023, that Defendants began notifying impacted individuals that an unauthorized actor had gained access to highly sensitive personal information from the Fallon archival data between February 27, 2023 and April 22, 2023 (the "Data Breach"). Included in the Data Breach were patient names, protected health information, and Social Security Numbers (SSNs) (collectively, the "Private Information").

4. Before ceasing operations in December 2022, Fallon provided emergency care to thousands of patients. By absorbing Fallon's employees and operations into its organization, Coastal became one of largest medical transportation providers in the New England region.

5. Defendants' positions as preeminent health organizations that hold a wide range of patient information meant that Defendants should have known how to prevent a data breach, and/or mitigate harm from such a breach. Defendants had a heightened duty to protect Plaintiff's and other Class members' data.

6. Defendants' security failures enabled the hackers to steal the Private Information of Plaintiff and other members of the Class—defined below. These failures put Plaintiff's and other Class members' Private Information at a serious, immediate, and ongoing risk. Additionally, Defendants' failures caused costs and expenses associated with the time spent and the loss of productivity from taking time to address and attempt to ameliorate the release of personal data. Mitigating and dealing with the actual and future consequences of the Data Breach has also created a number of future consequences for Plaintiff and Class members—including, as appropriate, reviewing records of fraudulent charges for services billed but not received, purchasing credit monitoring and identity theft protection services, the imposition of withdrawal and purchase limits

on compromised accounts, initiating and monitoring credit freezes, the loss of property value of their Private Information, and the stress, nuisance, and aggravation of dealing with all issues resulting from the Data Breach.

7. The Data Breach, which impacted at least 911,757 individuals, was caused and enabled by Defendants' violation of their obligations to abide by best practices and industry standards concerning the security of patients' records and private information. Defendants failed to comply with security standards and allowed their patients' Private Information to be compromised, which could have been prevented or mitigated after the Data Breach occurred.

8. Accordingly, Plaintiff asserts claims for: negligence; breach of implied contract; unjust enrichment/quasi-contract; and breach of fiduciary duty; and seeks injunctive relief, monetary damages, and statutory damages, as well as all other relief as authorized in equity or by law.

JURISDICTION AND VENUE

9. Jurisdiction of this Court is founded upon 28 U.S.C. § 1332(d) because the matter in controversy exceeds the value of $5,000,000, exclusive of interests and costs, there are more than 100 class members, and the matter is a class action in which any member of a class of plaintiffs is a citizen of a different state from any Defendants.

10. This Court has personal jurisdiction over this action because Defendants are headquartered in Massachusetts and have thus availed themselves of the rights and benefits of the Commonwealth of Massachusetts by engaging in activities including (i) directly and/or through their parent company, affiliates and/or agents providing services throughout the United States and in this judicial district and abroad; (ii) conducting substantial business in this forum; (iii) having a registered agent to accept service of process in the Commonwealth of

Massachusetts; and/or (iv) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided in Massachusetts and in this judicial District.

11. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendants maintain places of business within this District and have purposefully engaged in activities, including transacting business in this District and engaging in the acts and omissions alleged herein, in this District.

PARTIES

A. Plaintiff Daniel Durgin

12. Plaintiff Daniel Durgin is a citizen of Massachusetts and resides in Boston.

13. Mr. Durgin received emergency medical services from Fallon Ambulance Service when it operated prior to its cessation of operations in December 2022.

14. In order to receive emergency medical transport from Fallon, Plaintiff Durgin was required to disclose his Private Information, which was then entered into Fallon's database and maintained by Defendants.

15. In maintaining Mr. Durgin's Private Information, Defendants expressly and impliedly promised to safeguard it. Defendants, however, did not take proper care of Mr. Durgin's Private Information, leading to its exposure as a direct result of Defendants' inadequate security measures.

16. In December of 2023, Plaintiff Durgin received a notification letter from Transformative alerting him to the fact of the Data Breach and that his Private Information was accessed by cybercriminals.

17. The letter also offered two years of credit monitoring, which was and continues to be insufficient for Durgin and the other Class members.

18. In the months and years following the Data Breach, Mr. Durgin and the other Class members will experience a slew of harms because of Defendants' ineffective data security measures. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, targeted advertising without patient consent, and emotional distress.

19. Plaintiff Durgin greatly values his privacy, especially in receiving medical services, and would not have paid the amount that he did for services if he had known that his information would be maintained using inadequate data security systems.

B. Defendants

20. Defendant Transformative is a limited liability corporation organized under the laws of the Commonwealth of Massachusetts. Transformative has a principal place of business at 275 Grove Street, Ste. 2-400, Newton, Massachusetts.

21. Defendant Coastal is a limited liability corporation organized under the laws of the Commonwealth of Massachusetts. Coastal has a principal place of business at 372 Yarmouth Road, Hyannis, Massachusetts.

22. Fallon Ambulance Service was a subsidiary of Transformative until September 2022, when Transformative agreed to sell Fallon to Coastal in an acquisition.

23. By December 2022, Coastal had absorbed Fallon's employees and operations into its company structure, including rebranding Fallon's ambulances with Coastal's logo. Fallon no longer exists as a corporate entity.

24. Both Defendants' corporate policies and practices, including those used for data privacy, are established in, and emanate from, the Commonwealth of Massachusetts.

FACTS

25. Fallon provided emergency medical services to thousands of patients per year. Through their administration of those services as parent companies, Defendants stored and continue to store a vast amount of patients' Private Information. In doing so, Defendants were entrusted with, and obligated to safeguard and protect, the Private Information of Plaintiff and the Class in accordance with all applicable laws.

26. On April 21, 2023, Defendants were alerted that an unauthorized third party accessed the archival data from Fallon's computer network.

27. In December of 2023, Plaintiff Durgin received a notification letter from Transformative. The letter reads, in part, as follows:

> We are contacting you to provide information regarding a security incident at Fallon Ambulance Service ("Fallon") that may have impacted some of your information and to inform you about steps you may take to help protect your information. Fallon was a medical transportation company that, in part, responded to patient emergencies in the greater Boston area and provided administrative services for affiliated medical transportation companies. Fallon ceased operations in December 2022 but, to comply with legal obligations, has maintained an archived copy of data previously stored on its computer systems.
>
> **What Happened:** On or around April 21, 2023, after Fallon had ceased operations, we detected suspicious activity within our data storage archive. We promptly took steps to secure the archive and initiated a comprehensive investigation into the matter with the assistance of third-party specialists. After an extensive review of the event, we identified that the activity appears to have occurred as early as February 17, 2023 through April 22, 2023 and that files were obtained by an unauthorized party that may have contained personal information. We then conducted a comprehensive evaluation of the potentially impacted files to determine the nature of any personal information contained therein and to identify the current mailing address for potentially impacted individuals. This process was completed on or around December 27, 2023. Based on our review, we determined that the impacted files may have included certain of your personal information. While we currently have no evidence of identity theft or fraud related to your

> information as a result of this matter, we are notifying you to provide you with information and steps you can take to help protect your information.

28. The Data Breach occurred because Defendants failed to take reasonable measures to protect the Private Information they collected and stored. Among other things, Defendants failed to implement data security measures designed to prevent this attack, despite repeated public warnings to the healthcare industry about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past. Defendants did not properly contain patient health data, which requires a heightened level of protection. Defendants failed to disclose to Plaintiff and Class members the material fact that they did not have adequate data security practices to safeguard customers' personal data, and in fact falsely represented that their security measures were sufficient to protect the Private Information in their possession.

29. Had Plaintiff known that his data would be stored with improper security measures, he would have reevaluated what information he chose to provide to Fallon, which collected and stored the data of thousands of patients or sought another provider of emergency medical services.

30. Defendants' failure to provide immediate formal notice of the Breach to Plaintiff and Class members, and their delay of several months in providing notice, exacerbated the injuries resulting from the Data Breach.

A. Defendants Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Patients' Private Information, Despite a Rise in Data Breaches Affecting the Healthcare Industry

31. Defendants were aware of or should have been aware of the risk of data breaches in the healthcare industry, which has had well-publicized breaches from misuse or misconfigurations over the past four years.

32. Defendants operate major regional healthcare services, yet Defendants did not allocate adequate resources for cybersecurity protection of patient information.

33. Under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Defendants had a heightened duty to protect patient Private Information.

34. Defendants failed to ensure that proper data security safeguards were being implemented throughout the breach period.

35. Defendants failed to ensure that their healthcare operations would not be impacted in case of a data breach.

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

37. Plaintiff and Class members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants and any of their affiliates would comply with their obligations to keep such information confidential and secure from unauthorized access.

38. Defendants' failure to provide adequate security measures to safeguard patients' Private Information is especially egregious because Defendants operate in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to patients' highly confidential Private Information.

39. Ponemon Institute, an expert in the annual state of cybersecurity, has indicated that healthcare institutions were the top target for cyber-attacks in 2020.[1]

40. In fact, Defendants have been on notice for years that the medical industry is a prime target for scammers because of the amount of confidential patient information maintained.

[1] IBM Security, *Cost of a Data Breach Report*, PONEMON INST. 5 (2020), https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.

In 2019 alone, numerous entities in the healthcare sector suffered high-profile data breaches, including Quest Diagnostics and LabCorp.

B. Defendants' Data Security and HIPAA Violations

41. Defendants' data security lapses demonstrate that they did not honor their duties to protect patient information by failing to:

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

ii. Adequately protect patients' Private Information;

iii. Properly maintain their own data security systems for existing intrusions;

iv. Ensure that they employed reasonable data security procedures;

v. Ensure the confidentiality and integrity of electronically maintained private health information ("PHI") they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

vii. Implement 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);

viii. Protect 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);

ix. Protect 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);

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

xi. Train 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).

C. Damages to Plaintiff and the Class

42. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Data Breach.

43. The information obtained by hackers and scammers is an extremely valuable commodity that is commonly traded on the black market and results in the diminishment of the value of a person's electronic presence years into the future when it is misused.

44. Plaintiff and the Class have experienced or currently face a substantial risk of out-of-pocket fraud losses such as loss of funds from bank accounts, medical fraud and/or identity theft, fraudulent charges on credit cards, targeted advertising, suspicious phones calls, and similar identity theft.

45. Plaintiff and Class members have also incurred out of pocket costs for protective measures such as credit freezes or payment for phone scam detection.

46. Plaintiff and Class members suffered a loss of the property value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have

recognized the propriety of the loss of the property value of personal information in data breach cases.

47. Class members who paid Fallon or Defendants for their services were also damaged via "benefit of the bargain" damages. Such members of the Class 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 Fallon or Defendants was intended to be used by Fallon or Defendants to fund adequate data security. Defendants did not properly comply with their data security obligations. Thus, the Class members did not get what they paid for.

48. Members of the Class have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

49. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.

50. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[2]

51. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, loans, or even giving false information to police during an arrest.

[2] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number[.]" *Id.*

In the medical context, Private Information can be used to submit false insurance claims, obtain prescription drugs or medical devices for black-market resale, or get medical treatment in the victim's name. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers and will need to monitor their credit and tax filings for an indefinite duration.

52. 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 it failed to properly prepare for that risk.

D. The Value of Privacy Protections and Private Information

53. The fact that Plaintiff's and Class members' Private Information was stolen—and might presently be offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

54. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[3]

[3] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

55. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[4]

56. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[5]

57. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[6] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

58. Consumers place a high value not only on their highly confidential personal and medical information, but also on the privacy of that data. Researchers have begun to shed light on

---

[4] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, THE WALL STREET JOURNAL (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*] (last visited Oct. 1, 2021).

[5] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[6] *Web's Hot New Commodity*, *supra* note 10.

how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[7]

59. At relevant times, Defendants were well aware, or reasonably should have been aware, that the Private Information they maintain is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendants should have been particularly aware of these risks given the significant number of data breaches affecting the medical industry.

60. Had Defendants followed industry guidelines by adopting security measures recommended by experts in the field, Defendants would have prevented intrusion into their systems and, ultimately, the theft of patients' Private Information.

61. Given these facts, any institution that transacts business with patients and then compromises the privacy of patients' Private Information has thus deprived patients of the full monetary value of their transaction.

62. Due to damage from Defendants, Plaintiff and the other Class members now face a greater risk of continuous identity theft.

E. Duties and Responsibilities of Transformative and Coastal-Basis for Liability

63. After Fallon ceased operations in December 2022, Transformative retained an archived copy of data (including Plaintiff's and Class members' Private Information) that was previously stored on Fallon's computer systems. Transformative then maintained this data (including patients' Private Information) on its network.

64. While it maintained the Fallon archival data on its network, which it did at the time of the Data Breach, Transformative was responsible for securing, safeguarding, and maintaining the confidentiality of Plaintiff's and Class members' Private Information.

[7] *Victims of Identity Theft*, *supra* note 13, at 7.

65. During the period from February 17, 2023 through April 22, 2023, when the Data Breach took place, Transformative had a duty to secure, safeguard, and maintain the confidentiality of Plaintiff's and Class members' Private Information.

66. By failing to provide adequate security for Plaintiff's and Class members' Private Information, as stated in detail herein, Transformative breached that duty.

67. Transformative discovered the Data Breach on or about April 21, 2023, but did not provide notice to the affected individuals, including Plaintiffs and Class members, until more than eight months later, on December 27, 2023. By this conduct, Transformative breached its duty Plaintiffs and Class members to provide prompt notice of the Data Breach to affected persons. The existence of this duty is supported by, among other provisions, M.G.L., c. 93H, § 3.

68. After Coastal completed its acquisition of Fallon in December 2022, Fallon ceased to exist as an independent entity; Coastal absorbed Fallon's employees and operations into its corporate structure, including rebranding Fallon's ambulances with the Coastal name and logo.

69. At this point, and through at least the time of the Data Breach and its public disclosure, Coastal and its management maintained total control over Fallon's former employees and operations, and was responsible for all aspects of these operations, including providing adequate cyber-security.

70. In addition, through its acquisition of Fallon and the due diligence conducted in connection with the acquisition, Coastal knew that Fallon had possession of patients' Private Information and it knew that Fallon would and was required to maintain archival data, including

the Private Information, after it ceased operations. Coastal was also aware of Transformative's role in maintaining the Fallon archival data.

71. Because of this knowledge and because at the time of the Data Breach, Coastal was in control of Fallon's former employees and operations, Fallon had a duty to ensure that the Fallon archival data maintained by Transformative was properly and adequately secured and protected and that proper cyber-security measures were in place.

72. Coastal breached this duty, for the reasons alleged in detail herein.

CLASS ACTION ALLEGATIONS

73. Plaintiff brings all counts, as set forth below, individually and as a class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a nationwide Class defined as:

> All individuals who received a notice of data breach from Transformative Healthcare in or around December of 2023 (the "Class").

74. Excluded from the Class are Defendants and Defendants' affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff, and Counsel for the Parties and the members of their immediate family.

75. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

A. Numerosity—Fed. R. Civ. P. 23(a)(1)

76. The members of the Class are so numerous that joinder of all Class members would be impracticable. The Class is expected to number in the hundreds of thousands.

B. Commonality— Fed. R. Civ. P. 23(a)(2)

77. Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

i. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *inter alia*, HIPAA;

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

iii. Whether Defendants properly implemented their purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;

iv. Whether Defendants took reasonable measures to determine the extent of the Data Breach after they first learned about it;

v. Whether Defendants disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

vi. Whether Defendants' conduct constitutes breach of an implied contract;

vii. Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;

viii. Whether Defendants were unjustly enriched by their actions; and

ix. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief or other equitable relief, and the measure of such damages and relief.

C. Typicality—Fed. R. Civ. P. 23(a)(3).

78. Plaintiff's claims are typical of the claims of the other members of the Class because, *inter alia*, all Class members were similarly injured through Defendants' uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendants that are unique to Plaintiff.

D. Adequacy of Representation—Fed. R. Civ. P. 23(a)(4).

79. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class he seeks to represent, he has retained counsel competent and experienced in class action litigation and will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and his counsel.

E. Injunctive Relief—Fed. R. Civ. P. 23(b)(2).

80. Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declarative relief appropriate with respect to the Class under Rule 23(b)(2).

F. Superiority—Fed. R. Civ. P. 23(b)(3).

81. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be

impracticable for members of the Class to individually seek redress for Defendants' wrongful conduct. Even if members of the Class could afford individual litigation, the court system cannot. Individualized litigation creates a 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, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

82. Plaintiff fully incorporates by reference all of the above paragraphs, as though they are fully set forth herein.

83. Upon Defendants accepting and storing the Private Information of Plaintiff and the Class on their computer systems and on their networks, Defendants undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that the Private Information was private and confidential and should be protected as private and confidential.

84. Defendants owed a duty of care not to subject Plaintiff and the Class's Private Information to an unreasonable risk of exposure and theft, because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

85. Defendants owed numerous duties to Plaintiff and the Class, including the following:

i. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;

ii. To protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

iii. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

86. Defendants also breached their duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendants failed to provide adequate supervision and oversight of the Private Information with which they were and are entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

87. Defendants knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendants knew or should have known about numerous well-publicized data breaches within the medical industry.

88. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class members' Private Information.

89. Defendants breached their duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

90. Because Defendants knew that a breach of their systems would damage thousands of their customers, including Plaintiff and Class members, Defendants had a duty to adequately protect their data systems and the Private Information contained thereon.

91. Defendants' duty of care to use reasonable security measures arose because of the special relationship that existed between Defendants and their patients, which is recognized by laws and regulations including but not limited to HIPAA and 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.

92. 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.

93. 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.

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

95. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendants' misconduct included failing to: (1)

secure Plaintiff's and Class members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

96. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class members' Private 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:

i. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;

ii. Failing to adequately monitor the security of Defendants' networks and systems;

iii. Allowing unauthorized access to Class members' Private Information; and

iv. 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.

97. Through Defendants' acts and omissions described in this Complaint, including their failure to provide adequate security and their failure to protect Plaintiff's and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information during the time it was within Defendants' possession or control.

98. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to, failing to adequately protect the Private Information

and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

99. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

100. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class members suffered damages as alleged above.

101. Plaintiff and Class members are also entitled to injunctive relief requiring Defendants to, *inter alia*, (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 lifetime free credit monitoring to all Class members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and Class)

102. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

103. Through their course of conduct, Defendants, Plaintiff, and Class members entered into implied contracts for the provision of healthcare and data administration services, as well as implied contracts for the implementation of data security adequate to safeguard and protect the privacy of Plaintiff's and Class members' Private Information.

104. Specifically, Plaintiff and Class members entered into valid and enforceable implied contracts with Fallon when they first entered into contracts with Fallon to receive medical services. Defendants assumed and took on the obligations of Fallon under these implied contracts when Fallon ceased operations.

105. The valid and enforceable implied contracts to provide medical services that Fallon

entered into with Plaintiff and Class members (and that were later assumed by Defendants) include Defendants' promise to protect nonpublic Private Information given to Defendants or that Defendants created on their own from disclosure.

106. When Plaintiff and Class members provided their Private Information to Fallon in exchange for medical services, they entered into implied contracts pursuant to which Fallon, and subsequently Defendants, agreed to reasonably protect such Private Information.

107. Fallon solicited and invited Class members to provide their Private Information as part of Fallon's regular business practices. Plaintiff and Class members accepted Fallon's offers and provided their Private Information to Fallon. This Private Information was later maintained by or under the control of Defendants, who assumed the obligation to secure and protect it.

108. Plaintiff and Class members have fully performed their obligations under these contracts.

109. By entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

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

111. Under these implied contracts, Defendants was obligated to: (a) provide medical services to Plaintiff and Class members; and (b) protect Plaintiff and Class members' Private Information provided to obtain the benefits of such services. In exchange, Plaintiff and members of the Class agreed to pay money for these services, and to turn over their Private Information.

112. Both the provision of medical services and the protection of Plaintiff and Class

members' Private Information were material aspects of these implied contracts.

113. The implied contracts for the provision of medical services include the contractual obligations to maintain the privacy of Plaintiff and Class members' Private Information, which are also acknowledged, memorialized, and embodied in multiple documents (including, among other documents, Defendants' Data Breach notification letter).

114. Consumers of medical services value their privacy, the privacy of their dependents, and the ability to keep confidential their Private Information associated with obtaining such services. Plaintiff and Class members would not have entrusted their Private Information to Defendants and entered into these implied contracts with Defendants without an understanding that their Private Information would be safeguarded and protected; nor would they have entrusted their Private Information to Defendants in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

115. A meeting of the minds occurred as Plaintiff and Class members agreed and provided their Private Information to Defendants and paid for the provided services in exchange for, among other things, both the provision of healthcare and the protection of their Private Information.

116. Plaintiff and Class members performed their obligations under the contract when they paid for Defendants' services and/or provided Defendants with their Private Information.

117. Defendants materially breached their contractual obligation to protect the nonpublic Private Information Defendants gathered when the Private Information was accessed and exfiltrated through the Data Breach.

118. Defendants materially breached the terms of these implied contracts. Defendants did not maintain the privacy of Plaintiff and Class members' Private Information as evidenced by

their notifications of the Data Breach to Plaintiff and Class members. Specifically, Defendants did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA or HIPAA, or otherwise protect Plaintiff and Class members' private information as set forth above.

119. The Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

120. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiff and Class members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and Class members, therefore, were damaged in an amount at least equal to the difference in the value between the healthcare with data security protection they paid for and the healthcare they received.

121. Had Defendants disclosed that their data security was inadequate or that they did not adhere to industry-standard security measures, neither the Plaintiff, Class members, nor any reasonable person would have gone to Defendants to obtain healthcare services.

122. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out of pocket expenses to mitigate the effects of the Data Breach, including time lost responding to the Breach, and the loss of the benefit of the bargain they struck with Defendants.

123. Plaintiff and Class members are entitled to compensatory and consequential

damages suffered as a result of the Data Breach.

124. 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 adequate credit monitoring to all Class members.

COUNT III
Unjust Enrichment/Quasi-Contract
(On Behalf of Plaintiff and the Class)

125. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

126. Plaintiff brings this claim in the alternative to his breach of implied contract claim.

127. Plaintiff and Class members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and provided Defendants with their Private Information. In exchange, Plaintiff and Class members should have received from Defendants the goods and services that were the subject of the transaction and should have been entitled to have Defendants protect their Private Information with adequate data security.

128. Defendants knew that Plaintiff and Class members conferred a benefit on Defendants and have accepted or retained that benefit. Defendants profited from Plaintiff's purchases and used Plaintiff's and Class members' Private Information for business purposes.

129. Defendants failed to secure Plaintiff's and Class members' Private Information and, therefore, did not fully compensate Plaintiff and Class members for the value that their Private Information provided.

130. Defendants acquired the Private Information through inequitable means as it failed to disclose the inadequate security practices previously alleged.

131. If Plaintiff and Class members knew that Defendants would not secure their Private Information using adequate security, they would have made alternative healthcare choices that excluded Defendants.

132. Plaintiff and Class members have no adequate remedy at law.

133. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class members conferred on them.

134. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that it unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class members overpaid.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

135. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

136. Defendants had a fiduciary duty to safeguard patient Private information, which included that of Plaintiff and Class members.

137. Defendants breached this duty when they did not protect Plaintiff's and Class members' Private Information.

138. Defendants breached this duty when they did not provide adequate and timely notification of the Data Breach to Plaintiff and Class members.

139. Defendants breached their fiduciary duty when they violated 45 C.F.R. § 164.306(a)(1) by failing to ensure the confidentiality and integrity of Plaintiff's and Class member's protected and electronic health information that Defendants created, received,

maintained, and transmitted.

140. Defendants breached their fiduciary duty when they violated 45 C.F.R. § 164.312(a)(1) by failing to implement technical policies and procedures for their electronic information systems housing Private Information.

141. Defendants breached their fiduciary duty when they violated 45 C.F.R. § 164.308(a)(1) by failing to implement policies and procedures to prevent, detect, contain, and correct security violations.

142. Defendants breached their fiduciary duty when they violated 45 C.F.R. § 164.308(a)(6)(ii) by failing to mitigate, to the extent practicable, harmful effects of security incidents that were known to Defendants.

143. Defendants breached their fiduciary duty when they violated 45 C.F.R. § 164.306(a)(2) by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic Private Information.

144. Defendants breached their fiduciary duty when they violated 45 C.F.R. § 106.308(a)(6)(ii) by failing to mitigate harmful effects of security incidents known to Defendants.

145. Defendants breached their fiduciary duty when they violated 45 C.F.R. § 164.306(a)(2) by failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic Private Information.

146. Defendants violated 45 C.F.R. § 164.306(a)(3) when they failed to protect against reasonably anticipated uses or disclosures.

147. Defendants breached their fiduciary duty when they violated 45 C.F.R. § 164.530(b), and 45 C.F.R. § 164.308(a)(5) by failing to ensure that their workforce complied with HIPAA and failing to provide adequate training to their workforce.

148. Defendants breached their fiduciary duty when they violated 45 C.F.R. § 164.502 by impermissibly and improperly using and disclosing Private Information that remains accessible to unauthorized people.

149. Defendants breached their fiduciary duty when they violated 45 C.F.R. § 164.530(c) by failing to design, implement, and enforce policies and procedures to establish a physical administrative safeguard to protect Private Information.

150. Plaintiff and Class members face injuries as a direct and proximate result of Defendants' breaches of their fiduciary duties. These injuries include, but are not limited to:

i. Loss of control over Private Information;

ii. Compromise of Private Information;

iii. Lost opportunity costs associated with time spent to protect themselves and mitigate harm;

iv. Continued risk that Plaintiff's and Class members' Private Information could be stolen again;

v. Future costs associated with time spent protecting themselves from future harm;

vi. Diminished value of Defendants' services;

vii. Diminished value of Private Information;

viii. Anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VI
Declaratory Relief
(On Behalf of Plaintiff and the Class)

151. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully

set forth herein.

152. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the regulations described in this Complaint.

153. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class members' Private Information, and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

154. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect patient Private Information.

155. Defendants still possess the Private Information of Plaintiff and the Class.

156. Defendants have made no announcement that they have changed their data storage or security practices related to the Private Information.

157. Defendants have made no announcement or notification that they have remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

158. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach. The risk of another data breach is real, immediate, and substantial.

159. The hardship to Plaintiff and Class members if an injunction does not issue

exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs, Plaintiff and Class members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

160. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other patients whose Private Information would be further compromised.

161. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendants shall implement and maintain reasonable security measures, including but not limited to the following:

- engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on their systems on a periodic basis, and ordering them to promptly correct any problems or issues detected by such third-party security auditors;
- engaging third-party security auditors and internal personnel to run automated security monitoring;
- auditing, testing, and training their security personnel regarding any new or modified procedures;
- purging, deleting, and destroying Private Information not necessary for their provisions of services in a reasonably secure manner;
- conducting regular database scans and security checks; and
- routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully demands a jury trial of all issues so triable and requests that the Court enter judgment in their favor and against Defendants, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Class Counsel as requested in Plaintiff's expected motion for class certification;

B. Ordering Defendants to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

C. Ordering injunctive relief requiring Defendants to, *inter alia*, (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 indefinitely;

D. Ordering Defendants to pay attorneys' fees and litigation costs to Plaintiff and their counsel;

E. Ordering Defendants to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

F. Ordering Defendants to pay both pre- and post-judgment interest on any amounts awarded; and

G. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiff hereby requests trial by jury.

Date: January 18, 2024

Respectfully submitted,

/s/ David Pastor
David Pastor (BBO # 391000)
PASTOR LAW OFFICE, PC
63 Atlantic Avenue, 3rd Floor
Boston, MA 02110
Telephone No: (617) 742-9700
Email: dpastor@pastorlawoffice.com

Nicholas A. Migliaccio (*pro hac vice forthcoming*)
Jason Rathod (*pro hac vice forthcoming*)
MIGLIACCIO & RATHOD LLP
412 H Street NE
Washington, D.C. 20002
Telephone No: (202) 470-3520
Email: nmigliaccio@classlawdc.com

Plaintiffs' Counsel

ClassAction.org
