UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHSETTS

CELESTE BROWN and ROSS FINESMITH, on behalf of themselves and all others similarly situated, Plaintiffs, v. ALLCARE PLUS PHARMACY LLC, Defendant.	No. **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Celeste Brown and Ross Finesmith ("Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant AllCare Plus Pharmacy LLC, ("AllCare" or "Defendant") and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to their own actions, counsel's investigations, and facts of public record.

INTRODUCTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant is a Massachusetts based pharmaceutical company providing patient support services and specializing in complex medication management.

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together the "Protected Information"—about its current and former patients and employees. But Defendant lost control

over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. It is unknown precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to the Protected Information.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's Protected Information. In short, Defendant's failures placed the Class's Protected Information in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiffs are Data Breach victims having received breach notices from Defendant. They bring this class action on behalf of themselves, and all others harmed by Defendant's misconduct.

PARTIES

7. Plaintiff, Celeste Brown, is a natural person and citizen of North Carolina. She resides in Charlotte, North Carolina where she intends to remain.

8. Plaintiff, Ross Finesmith, is a natural person and citizen of New Jersey. He resides in Basking Ridge, New Jersey where he intends to remain.

9. Defendant, AllCare Plus Pharmacy LLC, is a Massachusetts limited liability company with its principal place of business located in Northborough, Massachusetts.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are over 100 putative Class Members.

11. This Court has personal jurisdiction over Defendant because it is headquartered in Massachusetts, regularly conducts business in Massachusetts, and Plaintiffs are citizens of a different state than Defendant, establishing minimal diversity jurisdiction.

12. Venue is proper in this Court under because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the Protected Information of Plaintiffs and the Class

13. Defendant is a Massachusetts based "recognized industry leader in patient support services" that provides "a full range of patient support services while specializing in complex medication management."[1]

14. As part of its business, Defendant receives and maintains the Protected Information of thousands of current and former patients and employees. In doing so, Defendant implicitly promises to safeguard their Protected Information in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their Protected Information.

15. Defendant clearly recognizes these duties as evidenced by the following statement on its Privacy Policy: "We pledge to protect the privacy of your health information as required by

[1] ALLCARE PLUS PHARMACY, Company Overview, https://allcareluspharmacy.com/about/ (last accessed June 22, 2023).

federal and state laws, regulations, and other applicable authorities…"[2] and "AllCare Plus Pharmacy's practice is dedicated to maintaining the privacy of our customer's PHI (Protected Health Information)…"[3]

16. Under state and federal law, businesses like Defendant have duties to protect patients' Protected Information and to notify them about breaches.

Defendant's Data Breach

17. Sometime on or before June 21, 2022, Defendant was hacked—exposing the Protected Information of Plaintiffs and the Class.[4] Defendant learned that a number of phishing emails were circulated to Defendant's employees. Defendant cannot even pinpoint the date they discovered the phishing emails were circulated, as the Notice of Data Breach merely states "Around June 21, 2022."[5]

18. Defendant does not know how long the hack actually lasted, other than stating their "investigation determined that an unauthorized party had accessed certain email inboxes of AllCare employes which contained personal information." Ultimately, these cybercriminals had access to Defendant's systems and Defendant had no idea when the hack began. The hack may have lasted for months.

19. Defendant admits that after "Further investigation determined that particular individuals had personal information included and potentially accessed in these mailboxes."[6]

[2] Privacy Policy, AllCare, https://allcarepluspharmacy.com/privacy/ (last accessed June 22, 2023).
[3] *Id.*
[4] *AllCare Plus Pharmacy Notice of Data Breach*, Attached hereto as **Exhibit A**.
[5] *Id.*
[6] *Id.*

20. Because of Defendant's Data Breach, at least the following types of Protected Information were compromised:

a. names;

b. address,

c. date of birth,

d. Social Security numbers;

e. Driver's license or other identification numbers,

f. financial account information; and

g. certain health information, including health insurance information and information about treatment and prescriptions.[7]

21. And yet, Defendant waited until March 13, 2023, before it began notifying the class—more than *eight months* after discovering the Data Breach.

22. Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

23. And when Defendant did notify Plaintiffs and the Class of the Data Breach, Defendant downplayed the seriousness of the Data Breach stating, "AllCare has not uncovered evidence that any personal information has been used for fraudulent or illicit purposes or has been made publicly available"[8]

[7] *Id.*
[8] *Id.*

24. Simply put, Defendant failed its duties when its inadequate security practices placed the sensitive Protected Information of Plaintiffs and Class Members into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class Members.

25. Still, Defendant declares that "Your trust is a top priority for AllCare, and we deeply regret the inconvenience this may cause" and "The privacy and protection of the personal information we maintain is a matter we take very seriously, and we have worked swiftly to resolve the incident."[9] Defendant failed to notify the class for eight months, so nothing Defendant claims to be doing regarding the Data Breach is being down swiftly. Regardless of how sincere Defendant's regrets are, Defendant's Data Breach caused widespread injury and monetary damages.

26. Since the Data Breach, Defendant declared that it is "implementing additional security measures, internal controls, and safeguards, as well as making changes to our policies and procedures to prevent a similar occurrence in the future."[10] But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

27. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Protected Information. And on information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

[9] *Id.*
[10] *Id.*

28. Defendant has done little to remedy its Data Breach. True, Defendant has offered concessions of credit monitoring to Plaintiffs and the Class[11], but upon information and belief, such services do not properly compensate Plaintiffs and the Class for the injuries that Defendant inflicted upon them.

29. Because of Defendant's Data Breach, the Protected Information of Plaintiffs and the Class were placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and the Class.

Plaintiff Celeste Brown's Experiences and Injuries

30. Plaintiff Celeste Brown is a former employee of Defendant. Ms. Brown was employed by Defendant for approximately three years from 2017 to 2020.

31. As a condition of her employment with Defendant, Ms. Brown provided Defendant with her Protected Information. Defendant used that Protected Information to facilitate its employment of Ms. Brown, including payroll, and required Ms. Brown to provide that Protected Information to obtain employment and payment for that employment.

32. In doing so, Ms. Brown trusted that Defendant would use reasonable measures to protect the Protected Information according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain her Protected Information and has a continuing legal duty and obligation to protect that Protected Information from unauthorized access and disclosure.

33. Ms. Brown received a Notice of Data Breach dated March 13, 2023.

[11] *Id.*

34. Ms. Brown has been the victim of identity theft, likely as a result of the Data Breach as she does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

35. Ms. Brown has had several fraudulent inquiries to her credit from June 2022 through November 2022.

36. Ms. Brown has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed her to take those steps in its breach notice.

37. Ms. Brown fears for her personal financial security and worries about what information was exposed in the Data Breach.

38. Because of Defendant's Data Breach, Ms. Brown has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, her injuries are precisely the type of injuries that the law contemplates and addresses.

39. Ms. Brown has suffered actual injury from the exposure (and likely theft) of her Protected Information—which violates her rights to privacy.

40. Ms. Brown has suffered actual injury in the form of damage to and diminution in the value of her Protected Information. After all, Protected Information is a form of intangible property—property that Defendant was required to adequately protect.

41. Ms. Brown has suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed her Protected Information right in the hands of criminals.

42. Because of the Data Breach, Ms. Brown anticipates spending considerable amounts of time and money to try and mitigate her injuries.

43. Today, Ms. Brown has a continuing interest in ensuring that her Protected Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Ross Finesmith's Experiences and Injuries

44. Plaintiff Ross Finesmith is unsure how Defendant obtained his Protected Information, but believes he previously received pharmaceutical services from Defendant, making him a former patient of Defendant.

45. As a condition of receiving prescriptions or Defendant's services, Defendant required Mr. Finesmith to provide it with his Protected Information.

46. Mr. Finesmith provided Defendant with his Protected Information in order to utilize the services of Defendant but would not have done so had he known that Defendant would not protect it as promised.

47. In May 2023, Mr. Finesmith became aware that his Protected Information was impacted by the Data Breach when he received Defendant's Notice of Data Breach.

48. Mr. Finesmith does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

49. Mr. Finesmith will continue to spend significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed him to take those steps in its breach notice.

50. Mr. Finesmith fears for his personal financial security and worries about what information was exposed in the Data Breach.

51. Because of Defendant's Data Breach, Mr. Finesmith has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, his injuries are precisely the type of injuries that the law contemplates and addresses.

52. Mr. Finesmith has suffered actual injury from the exposure (and likely theft) of his Protected Information—which violates his rights to privacy.

53. Mr. Finesmith has suffered actual injury in the form of damage to and diminution in the value of his Protected Information. After all, Protected Information is a form of intangible property—property that Defendant was required to adequately protect.

54. Mr. Finesmith has suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed his Protected Information right in the hands of criminals.

55. Because of the Data Breach, Mr. Finesmith anticipates spending considerable amounts of time and money to try and mitigate his injuries.

56. Today, Mr. Finesmith has a continuing interest in ensuring that his Protected Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

57. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their Protected Information is used;

b. diminution in value of their Protected Information;

c. compromise and continuing publication of their Protected Information;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen Protected Information; and

h. continued risk to their Protected Information —which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the Protected Information.

58. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

59. The value of Plaintiffs' and the Class's Protected Information on the black market is considerable. Stolen Protected Information trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

60. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell Protected Information far and wide.

61. One way that criminals profit from stolen Protected Information is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen Protected Information, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

62. The development of "Fullz" packages means that the Protected Information exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

63. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Protected Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other Class Members' stolen Protected Information is being misused, and that such misuse is fairly traceable to the Data Breach.

64. Defendant disclosed the Protected Information of Plaintiffs and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Protected Information of Plaintiffs and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

65. Defendant's failure to promptly and properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the

earliest ability to take appropriate measures to protect their Protected Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

66. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

67. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[12] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[13] Those 330 reported breaches exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[14]

68. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[15]

69. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[16]

70. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

---

[12] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.
[13] *Id*.
[14] *Id*.
[15] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.
[16] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited July 31, 2022).

Defendant Failed to Follow FTC Guidelines

71. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[17] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

73. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

74. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

[17] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

75. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to current and former patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

77. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

78. Other industry standard best practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

79. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

80. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Defendant Violated HIPAA

81. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[18]

82. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[19]

83. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

[18] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[19] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any 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);

d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement 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);

f. 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);

g. failing to identify and respond to suspected or known security incidents and failing to 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);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

84. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

85. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> **All individuals residing in the United States whose Protected Information was compromised in the Data Breach discovered by AllCare Plus Pharmacy LLC around June 21, 2022, including all those to received notice of the Data Breach.**

86. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

87. Plaintiffs reserve the right to amend the class definition.

88. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

89. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

90. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable.

91. Commonality and Predominance. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Protected Information;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant were negligent in maintaining, protecting, and securing Protected Information;

d. if Defendant breached contract promises to safeguard Plaintiffs' and the Class's Protected Information;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiffs and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

92. Typicality. Plaintiffs' claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

93. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class members' interests. And Plaintiffs have retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

94. Superiority. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

95. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

96. Plaintiffs and the Class entrusted their Protected Information to Defendant on the premise and with the understanding that Defendant would safeguard their Protected Information, use their Protected Information for business purposes only, and/or not disclose their Protected Information to unauthorized third parties.

97. Defendant owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry

standards for data security—would compromise their Protected Information in a data breach. And here, that foreseeable danger came to pass.

98. Defendant has full knowledge of the sensitivity of the Protected Information and the types of harm that Plaintiffs and the Class could and would suffer if their Protected Information was wrongfully disclosed.

99. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs' and Class Members' Protected Information.

100. Defendant owed—to Plaintiffs and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the Protected Information in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class Members within a reasonable timeframe of any breach to the security of their Protected Information.

101. Also, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their

Protected Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

102. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Protected Information it was no longer required to retain under applicable regulations.

103. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Protected Information of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

104. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Protected Information, a necessary part of employment and/or obtaining medical services from Defendant.

105. The risk that unauthorized persons would attempt to gain access to the Protected Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Protected Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Protected Information—whether by malware or otherwise.

106. Protected Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Protected Information of Plaintiffs' and Class Members' and the importance of exercising reasonable care in handling it.

107. Defendant improperly and inadequately safeguarded the Protected Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

108. Defendant breached these duties as evidenced by the Data Breach.

109. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' Protected Information by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the Protected Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

110. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the Protected Information of Plaintiffs and Class Members which actually and proximately caused the Data Breach and Plaintiffs' and Class Members' injury.

111. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class Members' injuries-in-fact.

112. Defendant has admitted that the Protected Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

113. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

114. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Protected Information by criminals, improper disclosure of their Protected Information, lost benefit of their

bargain, lost value of their Protected Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiffs and the Class)

115. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

116. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

117. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the Class Members' sensitive PII.

118. Defendant breached its respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

119. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

120. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

121. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiffs and Class Members would not have been injured.

122. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their Protected Information.

123. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiffs' and Class Members' PHI.

124. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed supra. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

125. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

126. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

127. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

128. Plaintiffs and Class Members were required to provide their Protected Information to Defendant as a condition of employment and/or receiving medical services provided by Defendant. Plaintiffs and Class Members provided their Protected Information to Defendant or its third-party agents in exchange for employment and/or Defendant's medical services and reasonably believed that the funds they paid, or services they provided, to Defendant included amounts towards protecting the security of their Protected Information.

129. Plaintiffs and the Class Members accepted Defendant's offers by disclosing their Protected Information to Defendant or its third-party agents in exchange for employment or medical services and by paying for those medical services.

130. In turn, and through internal policies, Defendant agreed to protect and not disclose the Protected Information to unauthorized persons.

131. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's Protected Information.

132. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their Protected Information

133. After all, Plaintiffs and Class Members would not have entrusted their Protected Information to Defendant or its third-party agents in the absence of such an agreement with Defendant.

134. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

135. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

136. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

137. Defendant materially breached the contracts it entered with Plaintiffs and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic Protected Information that Defendant created, received, maintained, and transmitted.

138. In these and other ways, Defendant violated its duty of good faith and fair dealing.

139. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed *supra*).

140. Plaintiffs and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

141. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

142. Given the relationship between Defendant and Plaintiffs and Class Members, where Defendant became guardian of Plaintiffs and Class Members' Protected Information, Defendant became a fiduciary by its undertaking and guardianship of the Protected Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Protected Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

143. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their Protected Information.

144. Because of the highly sensitive nature of the Protected Information, Plaintiffs and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain

their Protected Information had they known the reality of Defendant's inadequate data security practices.

145. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' Protected Information.

146. Defendant also breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

147. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

148. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

149. This claim is pleaded in the alternative to the breach of implied contract claim.

150. Plaintiffs and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from using their Protected Information in the form of employment, or to obtain payment and facilitate its provision of services.

151. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class Members. And Defendant benefited from receiving Plaintiffs' and Class Members' Protected Information, as this was used for employment and to obtain payment and facilitate its provision of services.

152. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Protected Information.

153. Instead of providing a reasonable level of security, or retention policies, which would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

154. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class Members' payment because Defendant failed to adequately protect their Protected Information.

155. Plaintiffs and Class Members have no adequate remedy at law.

156. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

SIXTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

157. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

158. 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 to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

159. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs allege that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

160. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class Members.

161. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

162. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

163. And if a second breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs' and Class Members' injuries.

164. If an injunction is not issued, the resulting hardship to Plaintiffs and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

165. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiffs, Class Members, and the public at large.

PRAYER FOR RELIEF

Plaintiffs and Class Members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;

D. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Dated: July 1, 2023

Respectfully submitted,

By: */s/ Anthony I. Paronich*
Anthony I. Paronich
Paronich Law, P.C.
350 Lincoln Street, Suite 2400
Hingham, MA 02043
(508) 221-1510
anthony@paronichlaw.com

/s/ Raina C. Borrelli
TURKE & STRAUSS LLP
Raina Borrelli (*pro hac vice to be filed*)
Samuel J. Strauss (*pro hac vice* to be filed)
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiffs and Proposed Class

ClassAction.org