COMMONWEALTH OF MASSACHUSETTS

NORFOLK, ss. SUPERIOR COURT

CIVIL ACTION NO: 2382cv0023

WILLIAM BISCAN, TENNIE KOMAR, and LISA SMITH, on Behalf of Themselves and All Others Similarly Situated, Plaintiffs, v. SHIELDS HEALTH CARE GROUP, INC. Defendant	CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Plaintiffs William Biscan, Tennie Komar, and Lisa Smith (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, allege as and for their Class Action Complaint, the following against Shields Health Care Group Inc. ("Shields" or "Defendant"), based upon their personal knowledge with respect to themselves and their own acts, and upon information and belief, upon their own investigation and the investigation of their counsel, as to all other matters, as follows:

I. INTRODUCTION

1. Shields provides MRI, PET/CT, and ambulatory surgical services to patients at more than 40 locations throughout New England. Prior to and at the time of the cybersecurity breach compromising Plaintiffs and the proposed class, Shields provided healthcare services in Massachusetts.

2. This class action arises out of a targeted, intentional cyber-attack at Defendant's medical facilities that allowed third party criminal hackers to access and Defendant's computer systems and exfiltrate patient data from approximately March 7, 2022 to March 21, 2022, publicly

exposing the highly sensitive information and medical records of approximately two million patients from Defendant's computer network ("the Data Breach").

3. Despite that Shields became aware of the Data Breach by March 28, 2022,[1] it failed to notify Plaintiffs and the putative Class Members within 60 days as required by law.[2] Notably, Shields failed to notify Plaintiffs of the Data Breach for more than two months from its discovery of the same.

4. As a healthcare provider, Shields knowingly collected patient personally identifiable information ("PII"), and protected health information ("PHI") (collectively, "Private Information") in confidence, and has a resulting duty to secure, maintain, protect, and safeguard that Private Information against unauthorized access and disclosure through reasonable and adequate security measures.

5. PHI is considered "the most confidential and valuable type of [PII], irrevocable once breached."[3]

6. As a result of the Data Breach, Plaintiffs and Class Members suffered ascertainable losses, including but not limited to, a diminution in the value of their private and confidential information, the loss of the benefit of their contractual bargain with Defendant, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

---

[1] *Notice of Data Security Incident*, SHIELDS HEALTH CARE GRP. (July 25, 2022), https://shields.com/notice-of-data-security-incident/..

[2] *What is Considered Protected Health Information Under HIPAA?*, HIPAA J. (Jan. 1, 2023), https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.

[3] Junyuan Ke, et al., *My Data or My Health? Heterogenous Patient Responses to Healthcare Data Breach*, SSRN (Feb. 10, 2022), http://dx.doi.org/10.2139/ssrn.4029103.

7. Plaintiffs' and Class Members' sensitive and private personal information – entrusted to Defendant, its officials, and agents – was compromised, unlawfully accessed, and stolen due to the Data Breach. Information compromised in the Data Breach includes names, addresses, dates of birth, Social Security numbers, insurance information, medical record numbers, patient identification numbers, other protected health information defined by HIPPA, and other Private Information.[4]

8. Plaintiffs bring this class action lawsuit on behalf of all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information, for failing to provide timely and adequate notice to Plaintiffs and other Class Members of the unauthorized access to their Private Information by an unknown third-party, and for failing to provide timely and adequate notice of precisely what information was accessed and stolen.

9. Defendant breached its duty to Plaintiffs and Class Members by maintaining Plaintiffs' and the Class Members' Private Information in a negligent and reckless manner.

10. Upon information and belief, the means of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information were known and foreseeable risks to Defendant. Thus, Defendant was on notice that failing to take steps necessary

[4] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. §§1320d, *et seq.* ("HIPAA"), PHI is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. §160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Jan. 6, 2023).

to secure the Private Information from those risks left the Private Information in a dangerous and vulnerable condition.

11. Defendant, and its employees, failed to properly monitor the computer network and systems housing the Private Information.

12. Had Defendant properly monitored its property, it would have discovered the intrusion sooner or been able to wholly prevent it.

13. Exacerbating an already devastating privacy intrusion, Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and stored is now in the hands of data thieves.

14. Armed with the Private Information accessed in the Data Breach, data thieves have data from Shields allowing them to commit a variety of crimes, including credit/debit card fraud, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based upon their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

15. As a direct result of the Data Breach, Plaintiffs and Class Members have suffered fraud and identity theft in their financial accounts – including checking accounts connected to debit cards and checks used to pay invoices for services at Shields – and continue to be exposed to a heightened and imminent risk of fraud and identity theft, potentially for the rest of their lives. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

16. Plaintiffs and Class Members already have, and will continue to incur out-of-pocket costs for purchasing credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft.

17. As a direct and proximate result of the Data Breach and subsequent exposure of their Private Information, Plaintiffs and Class Members have suffered and will continue to suffer damages and economic losses in the form of lost time needed to take appropriate measures to avoid unauthorized and fraudulent charges, putting alerts on their credit files, and dealing with spam messages and emails received as a result of the Data Breach. Plaintiffs and Class Members have suffered and will continue to suffer an invasion of their property interest in their own Private Information such that they are entitled to damages from Defendant for unauthorized access to, theft of, and misuse of their Private Information. These harms are ongoing, and Plaintiffs and Class Members will suffer from future damages associated with the unauthorized use and misuse of their Private Information as thieves will continue to use the information to obtain money and credit in their names for several years.

18. Plaintiffs seek to remedy these harms on behalf of all similarly situated individuals whose Private Information was accessed and/or removed from Defendant's network during the Data Breach.

19. Accordingly, Plaintiffs bring this action, on behalf of themselves and all others similarly situated, against Defendant seeking redress for its unlawful conduct asserting claims for negligence, negligence *per se*, breach of express contract, breach of implied contract, negligent misrepresentation, breach of implied covenant of good faith and fair dealing, invasion of privacy by intrusion, breach of fiduciary duty, breach of confidence, unjust enrichment, violation of the

Massachusetts Consumer Protection Act, MASS. GEN. LAWS ch. 93A, §§1, *et seq.*, and violation of the Massachusetts Consumer Protection Act, MASS. GEN. LAWS ch. 214, §1B.

II. PARTIES

20. Plaintiff William Biscan is a resident of Essex County, Massachusetts. Plaintiff Biscan was a Shields patient during the time period relevant to the Data Breach. Mr. Biscan received letter notice from Shields that his Private Information was improperly exposed to unauthorized third parties.

21. Plaintiff Tennie Komar is a resident of Middlesex County, Massachusetts, and was a Shields patient during the time period relevant to the Data Breach. Plaintiff Komar received letter notice from Shields that her Private Information was improperly exposed to unauthorized third parties.

22. Plaintiff Lisa Smith is a resident of Worcester County, Massachusetts, and was a Shields patient during the time period relevant to the Data Breach. Plaintiff Smith became aware of the Data Breach on or around June 7, 2022, when Shields first disclosed the Data Breach to the public. Ms. Smith had moved her residence numerous times following her MRI at Shields and as a result, did not receive a Data Breach letter. After making numerous repeated requests from Shields to send her the Data Breach letter to date, Ms. Smith has not received the Data Breach letter. Ms. Smith has however received verbal confirmation from Shields that her Private Information was in fact part of the Data Breach.

23. Defendant Shields is a Massachusetts corporation with its principal place of business at 700 Congress Street, Quincy, Massachusetts 02169. Shields is a provider of health care that has more than 40 facilities throughout New England, offering MRI, PET/CT, and outpatient surgical services.

III. JURISDICTION AND VENUE

29. This Court has subject matter jurisdiction over this action under the Supreme Judicial Court Order regarding amount-in-controversy requirement under MASS. GEN. LAWS ch. ch. 212, §3. This is a civil action for money damages with no reasonable likelihood that the amount in controversy will be less than $50,000.

30. This Court has personal jurisdiction over Defendant because Shields is headquartered in Quincy, Massachusetts, has a usual place of business is in Quincy, Massachusetts, and it regularly conduct business in Quincy, Massachusetts.

31. Venue is proper in this Court under MASS. GEN. LAWS ch. 223, §8(4) because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from Norfolk County, Shields has its usual place of business in Norfolk County, and Defendant has caused harm to Class Members residing in Norfolk County.

IV. STATEMENT OF FACTS

A. Shields' Business

32. In 1972, Tom and Mary Shields owned and operated the Madalawn Nursing Home in Brockton, Massachusetts. Over the next 10 years, Tom and Mary established the largest regional dialysis center in New England and opened the first independent regional MRI center in 1986. Presently, Shields has more than 40 facilities throughout New England, offering MRI, PET/CT, and outpatient surgical services.

33. Due to the nature of its services, Shields stores patients' Private Information in its system. Shields accomplishes this by keeping the Private Information electronically, as evidenced by this Data Breach.

34. Patients demand security to safeguard their Private Information. As a healthcare provider, Shields is required to ensure that such private, personal information is not disclosed or

disseminated to unauthorized third parties without the patients' express, written consent, as further detailed below.

B. The Data Breach

35. Beginning on or around March 7, 2022 through March 21, 2022, unauthorized third party computer hackers accessed the computer system of Shields and acquired Plaintiffs' and Class Members' Private Information. The unauthorized third-party computer hackers maintained uninterrupted access to the Private Information of Shields' patients, including Plaintiffs and Class Members, for at least two weeks. The unauthorized third-party computer hackers exfiltrated the Private Information of Plaintiffs and Class Members from Shields' computer system and exposed the Private Information for sale to other cybercriminals.

36. After learning of the issue, Shields commenced an investigation. That investigation revealed that approximately two million patients, the majority of whom were Massachusetts citizens, were victims of the cybersecurity incident. The investigation further revealed that information accessed and taken by the hackers includes patients' names, medical information, information related to their use of Shields' services, Social Security numbers, and other Private Information that Shields collected and maintained.

37. Defendant did not inform patients of this Data Breach until June 7, 2022, in a press release stating that the following information had been breached:

> "Full name, Social Security number, date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient ID, and other medical or treatment information." ("Notice").[5]

38. The Notice disclosed that there had been unauthorized suspicious activity on its network between March 7, 2022, to March 21, 2022. Shields did not discover this until March 28,

[5] *Notice of Data Security Incident*, Shields Health Care Grp. (July 25, 2022), https://shields.com/notice-of-data-security-incident/.

2022. The Notice indicated that the "suspicious activity may have involved data compromise" and that Shields "immediately launched an investigation into this issue . . . ."[6]

39. The Notice further informed patients that:

> This investigation determined that an unknown actor gained access to certain Shields systems from March 7, 2022 to March 21, 2022. Furthermore, the investigation revealed that certain data was acquired by the unknown actor within that time frame. Although Shields had identified and investigated a security alert on or around March 18, 2022, data theft was not confirmed at that time.
>
> Shields takes the confidentiality, privacy, and security of information in our care seriously. Upon discovery, we took steps to secure our systems, including rebuilding certain systems, and conducted a thorough investigation to confirm the nature and scope of the activity and to determine who may be affected. Additionally, while we have safeguards in place to protect data in our care, we continue to review and further enhance these protections as part of our ongoing commitment to data security.[7]

40. It took Shields nearly three months after the Data Breach to inform Plaintiff and Class Members of the Data Breach, resulting in Plaintiff and Class Members suffering harm they otherwise may have been able to avoid had Shields announced the Data Breach sooner.

41. Shields' Notice of Data Breach was untimely and woefully deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, how unauthorized parties accessed its computer server, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach was a system-wide breach, whether servers storing information were accessed, and how many patients were affected by the Data Breach.

42. Given the intentional and criminal nature of the cybersecurity hack, Plaintiffs' and Class Members' Private Information is now for sale to criminals on the dark web; meaning unauthorized parties have accessed and viewed Plaintiff's and Class Members' unencrypted,

---

6 *Id.*

7 *Id.*

unredacted information, including name, date of birth, billing and insurance information, patient referral information, relevant medical records, diagnosis information, Social Security numbers, and more.

C. Plaintiffs' Experiences Following the Data Breach

William Biscan

43. Plaintiff William Biscan has been a patient of Shields for approximately three years.

44. On multiple occasions, Plaintiff Biscan has been required to provide his Private Information to Shields as a condition of his treatment.

45. Although Shields discovered the Data Breach on March 28, 2022, Plaintiff Biscan was not notified of the Data Breach until sometime after July 21, 2022.

46. According to the Notice of Security Incident dated July 21, 2022 (the "Data Breach Notice"), sent by Defendant Shields to Plaintiff Biscan, Plaintiff Biscan's personal information, which included his full name, home address, telephone number, email address, date of birth, patient ID number, medical record number, health insurance information, and other medical or treatment information, was exposed in the Data Breach, and Defendant Shields learned of same on March 28, 2022.

47. After receiving the Data Breach Notice, Plaintiff Biscan spent at least 5-10 hours dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including reviewing and monitoring his bank accounts, credit card accounts, and other online accounts, researching the potential impact of the Data Breach, dealing with fraudulent charges on his BJs credit card account, and receiving a significant increase in spam emails, calls and texts, all as a result of his Private Information being exposed in the Data Breach. Plaintiff Biscan intends to spend additional time and effort taking steps to protect his Private Information

in the future. Because of the Data Breach, Plaintiff Biscan spent valuable time he otherwise would have spent on other obligations.

48. Moreover, Plaintiff Biscan spent this time at Shields' direction. In the notice letter Plaintiff Biscan received, Shields encouraged Plaintiff to spend time mitigating his losses by "reviewing your account statements and monitoring your credit reports for suspicious activity or errors" and "to remain vigilant against incidents of identity theft and fraud[.]"

49. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Biscan faces, Shields offered him a two-year membership to credit monitoring services. However, the offer is inadequate because data breach victims commonly face many years of ongoing identity theft.

50. After the Data Breach, Plaintiff Biscan experienced identity fraud in the form of unauthorized charges on his BJ's Mastercard. As a result, he was required to obtain a new credit card from BJ's. However, BJ's was updating their system at the time and Mr. Biscan was forced to wait 6-8 weeks for his replacement card during which time he had to use another payment card for his purchases. As a result, Plaintiff Biscan, who heavily used his BJ's Mastercard to purchase gasoline, lost the benefits and discounts associated with his BJ's Mastercard, including a 10-20 cents per gallon discount on gasoline purchases and a 3% cash back discount. When he finally received his replacement card, Plaintiff Biscan drove to BJ's to retrieve the card. Plaintiff Biscan believes the fraudulent charge on his credit card is a result of the Data Breach given that it occurred relatively soon after the Data Breach.

51. Plaintiff Biscan's increased concerns are further enhanced by a significant increase in spam emails, calls, and texts that he received after receiving the Data Breach Notice, including texts at all times of the day.

52. Plaintiff Biscan has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Mr. Biscan otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

53. In addition, Plaintiff Biscan has suffered and will continue to suffer emotional distress as a result of the Data Breach and has increased concerns for the loss of his privacy, which he would not have suffered had Defendant Shields implemented the necessary and proper safeguards to protect its patients' Private Informationfrom theft.

54. The Private Informationthat was accessed by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Biscan would take, and continue to take, necessary measures to protect his Private Information.

55. Plaintiff Biscan has a continuing interest in ensuring that his Private Information, which, upon information and belief, remain in Shields' possession, is protected and safeguarded from further and future breaches.

56. Plaintiff Biscan suffered actual injury in the form of fraudulent charges to his BJ's Mastercard, lost benefits and discounts associated with his BJ's Mastercard for 6-8 weeks, and gas expended to go to BJ's to obtain his replacement card. In addition, Plaintiff Biscan suffered actual injury in the form of damages to and diminution of the value of Private Information – a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving medical services, which was compromised in and as a result of the Data Breach. Plaintiff Biscan has also suffered actual injury in the form of lost time by having to deal with the consequences of the Data Breach, including reviewing and monitoring his bank accounts, credit card accounts, and other online accounts, researching the potential impact of the Data Breach, dealing with fraudulent

charges on his BJ's credit card account, and receiving a significant increase in spam emails, calls and texts, all as a result of the Data Breach.

Tennie Komar

57. Plaintiff Tennie Komar has been a patient of Shields for approximately seven years. She has undergone imaging at various Shields facilities, including UMass Memorial and Emerson Hospital.

58. On multiple occasions, Plaintiff Komar has been required to provide her Private Informationto Shields as a condition of her treatment.

59. Although Shields discovered the Data Breach on March 28, 2022, Plaintiff Komar was not notified of the Data Breach until sometime after July 21, 2022.

60. According to the Notice of Security Incident dated July 21, 2022 (the "Data Breach Notice"), sent by Defendant Shields to Plaintiff Komar, Plaintiff Komar's personal information, which included her full name, home address, telephone number, date of birth, Social Security number, patient ID number, medical record number, physician name, health insurance information, and other medical or treatment information, was exposed in the Data Breach, and Defendant Shields learned of same on March 28, 2022.

61. After receiving the Data Breach Notice, Plaintiff Komar spent at least 5-6 hours dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including notifying her bank and portfolio manager about the breach, contacting her insurance company, researching the potential impact of the Data Breach, signing up for credit monitoring, increasing her identity protection insurance, and dealing with an influx of spam emails and pop-ups on her devices, all as a result of her Private Informationbeing exposed in the Data Breach. Plaintiff Komar intends to spend additional time and effort taking steps to protect her

Private Informationin the future. Because of the Data Breach, Plaintiff Komar spent valuable time she otherwise would have spent on other obligations.

62. Moreover, Plaintiff Komar spent this time at Shields' direction. In the notice letter Plaintiff Komar received, Shields encouraged Plaintiff to spend time mitigating her losses by "reviewing your account statements and monitoring your credit reports for suspicious activity or errors" and to "remain vigilant against incidents of identity theft and fraud."

63. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Komar faces, Shields offered her a two-year membership to credit monitoring services. However, the offer is inadequate because data breach victims commonly face many years of ongoing identity theft.

64. Plaintiff Komar's increased concerns are further enhanced by recent spam emails and pop-ups on her devices that she began receiving after she received the Data Breach Notice, requiring her to incur expenses to have her device cleaned up.

65. As a result of the Data Breach, Plaintiff Komar also increased her identity protection insurance from $25 to $48 per year for additional coverage.

66. Plaintiff Komar has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Ms. Komar otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

67. In addition, Plaintiff Komar has suffered and will continue to suffer emotional distress as a result of the Data Breach and has increased concerns for the loss of her privacy, which she would not have suffered had Defendant Shields implemented the necessary and proper safeguards to protect its patients' Private Information from theft.

68. The Private Information that was accessed by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. Indeed, Plaintiff Komar's Social Security number and highly sensitive confidential medical and health insurance information were exposed in the Data Breach. It was reasonable and expected that Plaintiff Komar would take, and continue to take, necessary measures to protect her Private Information.

69. Plaintiff Komar has a continuing interest in ensuring that her Private Information, which, upon information and belief, remain in Shields' possession, is protected and safeguarded from further and future breaches.

70. Plaintiff Komar suffered actual injury in the form of out-of-pocket expenses and damages to and diminution of the value of her Private Information – a form of intangible property that Plaintiff entrusted to Defendant for the purpose of receiving medical services, which was compromised in and as a result of the Data Breach. In addition, Plaintiff Komar has suffered actual injury in the form of lost time by having to deal with the consequences of the Data Breach, including notifying her bank and portfolio manager about the breach, contacting her insurance company, researching the potential impact of the Data Breach, signing up for credit monitoring, increasing her identity protection insurance, and dealing with an influx of spam emails and pop-ups on her device, all as a result of the Data Breach.

Lisa Smith

71. Plaintiff Lisa Smith has been a patient of Shields for approximately five years.

72. On multiple occasions, Plaintiff Smith has been required to provide her Private Information to Shields as a condition of her treatment.

73. Although Shields discovered the Data Breach on March 28, 2022, Plaintiff Smith became aware of the Data Breach on or about June 7, 2022, when Shields first disclosed the Data Breach to the public.

74. After the announcement by Shields of the Data Breach, Plaintiff Smith spent at least 110 hours dealing with the consequences of the Data Breach and continues to spend many hours dealing with the Data Breach, including reviewing and monitoring her bank accounts, credit card accounts, credit reports and other online accounts, researching the potential impact of the Data Breach, and dealing with suspicious activity in her email account, all as a result of her Private Information being exposed in the Data Breach. Plaintiff Smith intends to spend additional time and effort taking steps to protect her Private Information in the future. Because of the Data Breach, Plaintiff Smith spent valuable time she otherwise would have spent on other obligations.

75. Moreover, Plaintiff Smith spent this time at Shields' direction. Shields encouraged Plaintiff Smith to spend time mitigating her losses by "reviewing your account statements and monitoring your credit reports for suspicious activity or errors" and to "remain vigilant against incidents of identity theft and fraud."

76. Recognizing the present, immediate, and substantially increased risk of harm, Shields offered a two-year membership to credit monitoring services to those individuals who received a Data Breach notification letter. While the offer is inadequate because data breach victims commonly face many years of ongoing identity theft, Ms. Smith has not had the opportunity to sign up for these services offered by Shields.

77. Plaintiff Smith's increased concerns are further enhanced by recent suspicious activity in her email account, the same account she has used for her medical and banking related needs for the past 20 years. She received an unsolicited notification directing her to re-enter her

password but the recovery email on the notification was not the same account she uses as her recovery email and was unknown to her. As a result, Plaintiff Smith had to change her passwords on her medical portals and other online accounts including her bank accounts and other accounts where she stores financial information. Plaintiff Smith has also received numerous "phishing" phone calls, beginning in or around June 2022, from individuals claiming to be from parties claiming to be Social Security disability consultants. Ms. Smith spent at least an hour on hold with the Social Security Administration to confirm that there had been no disability claims filed on her behalf. Ms. Smith continues to receive a variety of similar phishing phone calls from robocall programs.

78. Plaintiff has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach. This is time Ms. Smith otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

79. In addition, Plaintiff Smith has suffered and will continue to suffer emotional distress as a result of the Data Breach and has increased concerns for the loss of her privacy, which she would not have suffered had Defendant Shields implemented the necessary and proper safeguards to protect its patients' Private Information from theft.

80. The Private Information that was accessed by an unknown actor was the kind of sensitive information that can be used to commit fraud and identity theft. It was reasonable and expected that Plaintiff Smith would take, and continue to take, necessary measures to protect her Private Information.

D. Shields' Privacy Policies

81. In Shields' Privacy Practice statement on its website at shields.com/privacy/ it states that it is their responsibility as a provider to "Maintain the privacy of your health information

as required by law." In addition, Shields states in its Notice of Data Security Incident on its website at shields.com/notice-of-data-security-incident/ that "Shields takes the confidentiality, privacy, and security of information in our care seriously."

82. Shields also describes how it may use and disclose medical information for each category of uses or disclosures, none of which provide it a right to expose patients' Private Information in the manner it was exposed to unauthorized third parties in the Data Breach.

83. By failing to protect Plaintiffs' and Class Members' Private Information, and by allowing the Data Breach to occur, Shields broke these promises to Plaintiff and Class Members.

E. The Healthcare Sector Is Particularly Susceptible to Cyberattacks

84. Defendant was on notice that companies in the healthcare industry were targets for cyberattacks especially since it was involved in the Accellion data breach.

85. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[8]

86. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security

[8] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

> of patients' health and financial information, but also patient access to care.[9]

87. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[10] In 2017, a new record high of 1,579 breaches were reported representing a 44.7% increase.[11] That trend continues.

88. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[12] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[13] Almost 50% of the victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the customers were never able to

---

[9] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

[10] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, CISION PR Newswire (Jan. 19, 2017), https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html.

[11] *2017 Annual Data Breach Year-End Review*, Identity Theft Res. Ctr.,https://www.idtheftcenter.org/wp-content/uploads/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf (last visited Jan. 6, 2023).

[12] *2018 End-of-Year Data Breach Report*, Identity Theft Res. Ctr., https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINALWEB-V2-2.pdf (last visited Jan. 6, 2022).

[13] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), available at https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[14]

89. Healthcare related data breaches have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82% of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[15] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[16]

90. As a healthcare provider, Shields knew, or should have known, the importance of safeguarding the patients' Private Information entrusted to it and of the foreseeable consequences if its data security systems were breached. This is especially true given its involvement in the Accellion data breach. This includes the significant costs that would be imposed on Shields' patients as a result of a breach. Shields failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

---

[14] *Id.*

[15] *2019 HIMSS Cybersecurity Survey, HIMSS,* https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Jan. 6, 2023).

[16] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, CHIEF HEALTHCARE EXEC. (Apr. 4, 2019), https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

F. Shields Acquires, Collects, and Stores Its Patients' Private Information

91. Shields acquires, collects, and stores a massive amount of its patients' protected health information and other personally identifiable data.

92. As a condition of engaging in health services, Shields requires that these patients entrust them with highly confidential Private Information.

93. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Shields assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

94. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information, and, as current and former patients, they relied on Shields to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

G. The Value of Private Information and the Effects of Unauthorized Disclosure

95. At all relevant times, Defendant was well aware that the Private Information it collects from Plaintiffs and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

96. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[17] Indeed, a robust "cyber black market" exists in

[17] *What to Know About Identity Theft*, FED. TRADE COMM'N, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Jan. 6, 2023).

which criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

97. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363 according to the Infosec Institute.[18]

98. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

99. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[19]

100. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more

---

[18] *Data Breaches: In the Healthcare Sector,* CTR. FOR INTERNET SEC., https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited Jan. 6, 2023).

[19] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

> difficult to detect, taking almost twice as long as normal identity theft.

101. The ramifications of Shields' failure to keep its patients' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

102. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

103. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[20] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[21]

104. As a healthcare provider, Shields knew, or should have known, the importance of safeguarding its patients' Private Information entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Shields' patients as a result of a breach. Shields failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

---

[20] *See Medical ID Theft Checklist, IdentityForce https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Jan. 6, 2023).*

[21] *The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches ("Potential Damages*"), Experian (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

H. Shields Failed to Comply with Healthcare Industry Standards

105. HHS's Office for Civil Rights notes:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[22]

106. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment, yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

107. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because the of value of the Private Information which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[23] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

108. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Shields chose to ignore them. These best practices were known, or should have been known by Shields, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

---

[22] *What is Considered Protected Health Information Under HIPAA?*, HIPAA J., (Jan. 1, 2023), https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.

[23] *See e.g., 10 Best Practices for Healthcare Security, INFOSEC (Sept. 27, 2016), https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref.*.

I. Cyber Criminals Have and Will Continue to Use Plaintiffs' and Class Members' PII for Nefarious Purposes

109. Plaintiffs' and Class members' highly sensitive PII is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can be used in a variety of ways for criminals to exploit Plaintiffs and the Class members and to profit off their misfortune and stolen information. The cybercriminals' motives for the Data Breach were purely nefarious and malicious in nature: their one goal was to access Paxton's systems in order to obtain valuable PII to sell on the dark web.

110. Every year, identity theft causes tens of billions of dollars of losses to victims in the United States.[24] For example, with the PII stolen in the Data Breach, including Social Security numbers and bank account information, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[25] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class members. Indeed, Brasher has already had an SBA loan fraudulently obtained in her name. Given the timing of the data breach and the fraudulent SBA loan, it is clear the Data Breach and the fraudulent SBA loan are causally connected.

111. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.

---

[24] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[25] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Credit.com (Nov. 2, 2017), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

112. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[26]

113. Hackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[27]

114. For instance, with a stolen Social Security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[28]

115. If cyber criminals manage to access financial information, health insurance information, and other personally sensitive data – as they did here – there is no limit to the amount of fraud to which Defendant may expose the Plaintiffs and Class members.

J. Plaintiffs and Class Members Suffered Damages

116. The ramifications of Shields' failure to keep patients' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[29]

---

[26] Ari Lazarus, *How fast will identity thieves use stolen info?*, Fed. Trade Comm'n (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-willidentity-thieves-use-stolen-info.

[27] Stolen Laptops Lead to Important HIPAA Settlements, U.S. Dep't of Health & Human Servs. (Apr. 22, 2014), https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

[28] *See, e.g., supra* note 25.

[29] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

117. In addition to their obligations under state laws and regulations, Defendant owed a common law duty to Plaintiffs and Class Members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

118. Defendant further owed and breached its duty to Plaintiffs and Class Members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

119. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiffs' and Class Members' Private Information as detailed above, and Plaintiffs are now at a heightened and increased risk of identity theft and fraud.

120. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

121. Other risks of identity theft include loans opened in the name of the victim, medical services billed in their name, utility bills opened in their name, tax return fraud, and credit card fraud.

122. Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in their agreements with Shields and they were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

123. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information has diminished in value.

124. The Private Information belonging to Plaintiffs and Class Members is private, private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiffs' or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

125. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

126. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect patient data.

127. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiffs' and Class Members' Private Information.

128. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

129. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[30]

130. Defendant's failure to adequately protect Plaintiffs' and Class Members' Private Information has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sit by and do nothing to assist those affected by the incident. Instead, as Shields' Data Breach Notice indicates, it is putting the burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

131. As a result of Defendant's failures to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

i. The compromise, publication, theft and/or unauthorized use of their Private Information;

ii. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

iii. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future

[30] Erika Harrell, & Lynn Langton, *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUST., OFF. OF JUST. PROGRAMS BUREAU OF JUST. STATS. (Dec. 2013), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

iv. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fail to undertake appropriate measures to protect the Private Information in their possession;

v. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and

vi. Anxiety and distress resulting from fear of misuse of their medical information.

132. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

K. Shields' Delay in Identifying & Reporting the Breach Caused Additional Harm

133. It is axiomatic that:

> The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[31]

134. Indeed, once a data breach has occurred:

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills, insurance invoices, and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because

[31] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, BUSINESS WIRE (Feb. 1, 2017), https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million.

> it wasn't reported, they can't take action to protect themselves (internal citations omitted).[32]

135. Although their Private Information was improperly exposed on or about March 7-21, 2022, Plaintiffs and Class Members were not notified of the Data Breach until June 2022, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

136. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiffs and Class Members has been driven even higher.

V. CLASS ALLEGATIONS

137. Plaintiffs brings this class action on behalf of themselves herself and on behalf of all others similarly situated pursuant to Rule 23(a) and 23(b) of the Massachusetts Rules of Civil Procedure.

138. Plaintiffs seek certification of the following Class:

> All Massachusetts citizens whose Private Information was compromised in the data breach of Shields' systems from approximately March 7, 2022 to March 21, 2022.

139. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

---

[32] Allen St. John, *The Data Breach Next Door*, CONSUMER REPORTS, (Jan. 31, 2019), https://www.consumerreports.org/data-theft/the-data-breach-next-door/.

140. Plaintiffs reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

141. Numerosity, Mass. R. Civ. P. 23(a)(1): The Class are so numerous that joinder of all members is impracticable. Defendant has identified more than two million patients and citizens of Massachusetts whose Private Information may have been improperly accessed in the Data Breach whose Private Information was compromised, and the Class are apparently identifiable within Defendant's records.

142. Commonality, Mass. R. Civ. P. 23(a)(2) and (b): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

i. Whether and when Defendant actually learned of the Data Breach and whether its response was adequate;

ii. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their Private Information;

iii. Whether Defendant breached that duty;

iv. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs and Class Members' Private Information;

v. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and Class Members' PII/PHI;

vi. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' PII/PHI secure and prevent loss or misuse of that Private Information;

vii. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

viii. Whether Defendant caused Plaintiffs' and Class Members' damages;

ix. Whether Defendant violated the law by failing to promptly notify Class that their Private Information had been compromised;

x. Whether Plaintiffs and the other Class Members are entitled to actual damages, credit monitoring, and other monetary relief;

xi. Whether Defendant violated common law and statutory claims alleged herein.

143. Typicality, Mass. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members, because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

144. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

145. Adequacy, Mass. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class and Sub-class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

146. Superiority and Manageability, Mass. R. Civ. P. 23(b): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the

controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

147. The nature of this action and the nature of laws available to Plaintiffs and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of each individual Class with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

148. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class and Sub-class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

149. Adequate notice can be given to Class and Sub-class Members directly using information maintained in Defendant's records.

150. Unless a Class-wide injunction is issued, Plaintiffs and Class Members remain at risk that Defendant will continue to fail to properly secure the Private Information of Plaintiffs and Class resulting in another data breach, continue to refuse to provide proper notification to Class Members regarding the Data Breach, and continue to act unlawfully as set forth in this Consolidated Class Action Complaint.

151. Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class as a whole is appropriate under Rule 23(b) of the Massachusetts Rules of Civil Procedure.

152. Likewise, particular issues under Rule 23(a)(2) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

i. Whether Defendant owed a legal duty to Plaintiffs and Class to exercise due care in collecting, storing, using, and safeguarding their Private Information;

ii. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

iii. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

iv. Whether 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; and

v. Whether Class Members are entitled to actual damages, additional credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

153. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

154. Defendant required Plaintiffs and Class Members to submit Private Information in order to obtain insurance coverage and/or to receive health care services.

155. Defendant knew, or should have known, of the risks inherent in collecting and storing the Private Information of Plaintiffs and Class Members.

156. As described above, Defendant owed duties of care to Plaintiffs and Class Members whose Private Information had been entrusted with Shields.

157. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

158. Defendant acted with wanton disregard for the security of Plaintiffs' and Class Members' Private Information. Defendant knew or should have known that Shields had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the Private Information in health care databases, such as Shields's.

159. A "special relationship" exists between Defendant and the Plaintiffs and Class Members. Shields entered into a "special relationship" with Plaintiffs and Class Members because Shields collected the Private Information of Plaintiffs and the Class Members and stored it in the Shields Database – information that Plaintiffs and the Class Members had been required to provide to Shields.

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

161. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known it was failing to meet its duties, and that Defendant's breach would of such duties cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

163. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

164. Pursuant to the Federal Trade Commission Act (15 U.S.C. §45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

165. Pursuant to HIPAA (42 U.S.C. §1302d, *et seq*.), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

166. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act (15 U.S.C. §45) and HIPAA (42 U.S.C. §1302d, *et seq*.), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

167. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

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

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

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

COUNT III
Breach of Express Contract
(On Behalf of Plaintiffs and the Class)

171. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

172. Plaintiffs and Class Members entered into written agreements with Defendant as part of the medical services Defendant provided to Plaintiffs and Class Members. The agreements involved a mutual exchange of consideration whereby Defendant provided these services in exchange for payment from Class Members, Class Members' insurance carriers, and/or government programs remitting payment on Class Members' behalf.

173. Plaintiffs and Class Members and/or their insurance carriers paid Defendant for its services and performed under these agreements.

174. Defendant's failure to protect Plaintiffs' and Class Members' Private Information constitutes a material breach of the terms of these agreements by Defendant.

175. As a direct and proximate result of Defendant's breaches of express contract, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

176. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

177. Plaintiffs and Class Members entered into an implied contract with Shields when they obtained health care services from Shields, for which they were required to provide their Private Information. The Private Information provided by Plaintiffs and Class Members to Shields was governed by and subject to Shields's privacy duties and policies.

178. Shields agreed to safeguard and protect the Private Information of Plaintiffs and Class Members and to timely and accurately notify them in the event that their PII or PHI was breached or otherwise compromised.

179. Plaintiffs and Class members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with industry standards. Plaintiffs and Class members believed that Shields would use part of the monies paid to Shields under the implied contracts to fund adequate and reasonable data security practices.

180. Plaintiffs and Class members would not have obtained health care services from Shields or provided and entrusted their Private Information to Defendant in the absence of the implied contract or implied terms between them and Shields. The safeguarding of the Private

Information of Plaintiffs and Class Members and prompt and sufficient notification of a breach was critical to realize the intent of the parties.

181. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Shields. Shields breached its implied contracts with Plaintiffs and Class members to protect their Private Information when it: (1) failed to have security protocols and measures in place to protect that information; (2) disclosed that information to unauthorized third parties; and (3) failed to provide timely and accurate notice that their Private Information was compromised as a result of the Shields Data Breach.

182. As a direct and proximate result of Shields's breaches of implied contract, Plaintiffs and Class members sustained actual losses and damages as described in detail above and are also entitled to recover nominal damages.

COUNT V
Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and the Class)

183. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

184. Plaintiffs and Class Members entered into valid, binding, and enforceable express or implied contracts with Shields, as alleged above.

185. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Shields would act fairly and in good faith in carrying out its contractual

obligations to take reasonable measures to protect Plaintiffs' and Class Members' Private Information and to comply with industry standards and federal and state laws and regulations.

186. A "special relationship" exists between Shields and the Plaintiffs and Class Members. Shields entered into a "special relationship" with Plaintiffs and Class Members who sought medical services or treatment at Shields facilities and, in doing so, entrusted Shields, pursuant to its requirements, with their Private Information.

187. Despite this special relationship with Plaintiff, Shields did not act in good faith and with fair dealing to protect Plaintiffs' and Class Members' Private Information.

188. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Shields.

189. Shields's failure to act in good faith in implementing the security measures required by the contracts denied Plaintiffs and Class Members the full benefit of their bargain, and instead they received health insurance and related services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiffs and Class Members were damaged in an amount at least equal to this overpayment.

190. Shields's failure to act in good faith in implementing the security measures required by the contracts also caused Plaintiffs and Class Members to suffer actual damages resulting from the theft of their Private Information and remain at imminent risk of suffering additional damages in the future.

191. Accordingly, Plaintiffs and Class Members have been injured as a result of Shields's breach of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT VI
Negligent Misrepresentation

(On Behalf of Plaintiffs and the Class)

192. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

193. Defendant negligently and recklessly misrepresented material facts, pertaining to the provision of health care services, to Plaintiffs and Class Members by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs' and Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft.

194. Defendant negligently and recklessly misrepresented material facts, pertaining to the provision of health care services, to Plaintiffs and Class Members by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs' and Class Members' Private Information.

195. Because of multiple warnings about the inadequacy of its data privacy and security practices, Defendant either knew or should have known that its representations were not true.

196. In reliance upon these misrepresentations, Plaintiffs and Class Members obtained health care services from Defendant.

197. Had Plaintiffs and Class Members, as reasonable persons, known of Defendant's inadequate data privacy and security practices, or that Defendant was failing to comply with the requirements of federal and state laws pertaining to the privacy and security of Plaintiffs' and Class Members' Private Information, they would not have purchased health services from Defendant, and would not have entrusted their Private Information to Defendant.

198. As direct and proximate consequence of Defendant's negligent misrepresentations, Plaintiffs and Class Members has suffered the injuries alleged above.

COUNT VII
Invasion of Privacy by Intrusion
(On Behalf of Plaintiffs and the Class)

199. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

200. Plaintiffs and Class Members had a reasonable expectation that Defendant would maintain the privacy of the Private Information collected and maintained by Shields.

201. Shields represented to Plaintiffs and Class Members that it would not disclose their Private Information except in a handful of clearly defined and disclosed circumstances.

202. Despite representations to the contrary, Defendant failed to protect and safeguard the Private Information entrusted to Shields by Plaintiffs and Class Members and in so doing intruded on the private and personal affairs of Plaintiffs and Class Members in a manner highly offensive to a reasonable person; invaded the privacy of Plaintiffs and Class Members by disclosing, without authorization, the PHI and PII of Plaintiffs and Class Members, inconsistent with both the purpose of the collection of the Private Information and inconsistent with the uses of said Private Information previously disclosed to Plaintiffs and Class Members; failed to provide sufficient security to protect the Private Information of Plaintiffs and Class Members from unauthorized access; enabled, by failing to protect it sufficiently, the disclosure of Private Information without the consent of Plaintiffs or Class Members.

203. Shields knew, or acted with reckless disregard in not knowing, that the Private Information collected from Plaintiffs and Class Members was, because of its nature, subject to a significant risk of unauthorized access.

204. Shields knew, or acted with reckless disregard in not knowing, that a reasonable person would consider its failure to adequately protect and secure their Private Information to be highly offensive.

205. Shields's disclosure of Plaintiffs' and Class Members' Private Information without their consent constituted a violation of the privacy of Plaintiffs and Class Members.

206. Shields's failure to provide sufficient security to protect the Private Information of Plaintiffs and Class Members, leading to unauthorized access to that data by unauthorized parties constituted the unlawful publication of that Private Information by Shields.

207. The Private Information disclosed in the Shields Data Breach was not generally known to the public and is not a matter of legitimate public concern.

208. Plaintiffs and Class Members had a reasonable expectation in the privacy of the Private Information that they provided to Shields. That reasonable expectation was thwarted by Defendant's actions and inactions and Defendant's conduct constituted an invasion of Plaintiffs' and Class Members' privacy.

209. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial as well as restitution and injunctive relief.

210. As direct and proximate consequence of Defendant's negligent misrepresentations, Plaintiffs and Class Members has suffered the injuries alleged above.

COUNT VIII
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

211. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

212. Defendant accepted the special confidence placed in it by Plaintiffs and Class Members, even asserting that it is "takes the confidentiality, privacy, and security of information in [its] care seriously" and by the promulgation of its Privacy Practice. There was an understanding between the parties that Defendant would act for the benefit of Plaintiffs and Class Members in preserving the confidentiality of the Private Information.

213. Defendant became the guardian of Plaintiffs' and the Class Members' Private Information and accepted a fiduciary duty to act primarily for the benefit of its patients, including Plaintiffs and the Class Members, including safeguarding Plaintiffs' and the Class Members' Private Information.

214. Defendant's fiduciary duty to act for the benefit of Plaintiffs and Class Members pertains as well to matters within the scope of its medical relationship with its patients, in particular, to keep secure the Private Information of those patients.

215. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to: (a) diligently discover, investigate, or give notice of the Data Breach in a reasonable and practicable period of time; (b) encrypt and otherwise protect the integrity of its computer systems containing Plaintiffs' and the Class Members' Private Information; (c) timely notify and/or warn them of the Shields Data Breach; (d) ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. §164.306(a)(1); (e) 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) implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. §164.308(a)(1); (g) identify and respond to suspected or known security incidents and 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) 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); (i) 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); (j) ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 C.F.R. §164.306(a)(94); (k) effectively train all members of its workforce (including independent contractors) on the policies and procedures necessary to maintain the security of PHI, in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. § 164.308(a)(5); (l) design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in violation of 45 C.F.R. §164.530(c); and (m) by otherwise failing to safeguard Plaintiffs' and the Class Members' Private Information.

216. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Shields Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms

of time, effort, and money that will be expended as result of the Shields Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

217. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IX
Breach of Confidence
(On Behalf of Plaintiffs and the Class)

218. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

219. At all times during Plaintiffs' and the Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and the Class Members' Private Information that Plaintiffs and the Class Members provided to Defendant.

220. As alleged herein and above, Defendant's relationship with Plaintiffs and the Class Members was governed by terms and expectations that Plaintiffs' and the Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

221. Plaintiffs and the Class Members receiving treatment from Defendant provided Plaintiffs' and the Class Members' Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

222. Plaintiffs and the Class Members receiving treatment from Defendant also provided Plaintiffs' and the Class Members' Private Information to Defendant with the explicit and implicit

understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

223. Defendant voluntarily received in confidence Plaintiffs' and the Class Members' Private Information with the understanding that information would not be disclosed or disseminated to the public or any unauthorized third parties.

224. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and the Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and the Class Members' confidence, and without their express permission.

225. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and the Class Members have suffered damages.

226. But for Defendant's disclosure of Plaintiff's and the Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and the Class Members' Private Information as well as the resulting damages.

227. The injury and harm Plaintiffs and the Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and the Class Members' Private Information. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and the Class Members' Private Information.

228. As a direct and proximate result of Defendant's breach of its confidence with Plaintiffs and the Class Members, Plaintiffs and the Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of current and former patients; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class Members.

229. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and the Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT X
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

230. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

231. Under MASS. GEN. LAWS ch. 231A, §1, this Court is authorized to make binding declarations of right, duty, status, and other legal relations either before or after a breach or violation has occurred in any case in which an actual controversy has arisen.

232. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' Private Information and whether Shields is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information. Plaintiffs allege that Shields's data security measures remain inadequate. Furthermore, Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their PII and/or PHI will occur in the future.

233. Pursuant to its authority under MASS. GEN. LAWS ch. 231A, §1, this Court should enter a judgment declaring, among other things, the following:

234. Shields owes a legal duty to secure patients' Private Information and to timely notify patients of a data breach under the common law, Section 5 of the FTC Act and HIPAA.

235. Shields breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

236. This Court also should issue corresponding prospective injunctive relief requiring Shields to employ adequate security protocols consistent with law and industry standards to protect patients' Private Information.

237. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Shields. The risk of another such breach is real, immediate, and substantial. If another breach at Shields occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

238. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Shields if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Shields of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Shields has a pre-existing legal obligation to employ such measures.

239. 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 at Shields, thus eliminating the additional injuries that would result to Plaintiffs, Class Members, and consumers whose confidential information would be further compromised.

COUNT XI
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

240. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

241. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of payments made for the purchase of health care services.

242. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

243. The payments for healthcare services that Plaintiffs and Class Members paid (directly or indirectly) to Defendant should have been used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

244. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between the health care services with the reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and the inadequate health care services without reasonable data privacy and security practices and procedures that they received.

245. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by HIPAA regulations, federal, state and local laws, and industry standards.

246. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by Defendant.

247. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendant traceable to Plaintiffs and Class Members.

COUNT XII

Violation of the Massachusetts Consumer Protection Act, MASS. GEN. LAWS ch. 93A, §§1, *et seq*.

(On Behalf of Plaintiffs and the Class)

248. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

249. Defendant is a natural person, corporation, trust, partnership, incorporated or unincorporated association, or another legal entity.

250. Defendant is engaged in advertising, the offering for sale, rent or lease, the sale, rent, lease or distribution of any services and any property, tangible or intangible, real, personal or mixed, any security and any contract of sale of a commodity for future delivery, and any other article, commodity, or thing of value wherever situated.

251. Defendant is engaged in trade or commerce directly or indirectly affecting the people of the state of Massachusetts.

252. Defendant has engaged in unfair or deceptive acts or practices in the conduct of trade or commerce.

253. Defendant misrepresented that it would keep the Private Information of Plaintiffs and the Massachusetts Sub-Class members secure, private, and confidential.

254. Defendant had a duty to keep the Private Information safe and secure under HIPPA and regulations promulgated thereunder, the FTCA and regulations promulgated thereunder, and MA. GEN. LAWS 93H, §2 and regulations promulgated thereunder.

255. Defendant failed to adequately protect and secure the Private Information.

256. Defendant failed to comply with its obligations to protect and secure the Private Information under HIPPA and regulations promulgated thereunder, the FTCA and regulations promulgated thereunder, and MASS. GEN. LAWS ch. 93H, §2 and regulations promulgated thereunder.

257. Defendant failed to comply with industry standards for the protection and security of the Private Information.

258. Defendant failed to comply with its own privacy practice relating to the protection and security of the Private Information.

259. Criminals were able to access the Private Information through a data breach.

260. Defendant had a duty to timely notify patients, including Plaintiffs and the Class, of the data breach under 45 C.F.R. §164.404 and MASS. GEN. LAWS ch. 93H, §3.

261. Although it was aware of the data breach, Defendant failed to timely notify its patients of the data breach, including the members of the Class.

262. The aforementioned actions and omissions constitute unfair or deceptive acts or practices.

263. As a result of the aforementioned actions and omissions, Plaintiffs and the Class have suffered, and will continue to suffer, injury in an amount to be determined at trial, including, but not limited to: the loss of the benefit of their bargain with Defendant; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses incurred protecting themselves from fraudulent activity; loss of value of their Private Information; and an increased, imminent risk of fraud and identity theft.

264. As a result of the aforementioned actions and omissions, Plaintiffs and the Class seek their actual damages, statutory damages, treble damages, punitive damages, their costs and reasonable attorneys' fees, and any injunctive or equitable relief needed to secure Private Information in the possession, custody, and control of Defendant and its agents.

265. A notice identifying the claimant and reasonably describing the unfair or deceptive act or practice relied upon and the injury suffered was mailed or delivered to Defendant at least thirty days prior to the filing of a pleading alleging this claim for relief.

COUNT XV
Violation of the Massachusetts Consumer Protection Act, MASS. GEN. LAWS ch. 214, §1B (On Behalf of Plaintiffs and the Class)

266. Plaintiffs repeat and reallege all allegations set forth above as if they were fully set forth herein.

267. Defendant is a natural person, corporation, trust, partnership, incorporated or unincorporated association, or another legal entity.

268. Defendant had a legal duty to adequately safeguard Plaintiff's and Class Members' Private Information.

269. Defendant had a legal duty to ensure that Plaintiff's and Class Member's Private Information was not made public or disclosed to third parties without prior authorization.

270. Defendant had a legal duty to ensure that its agents and employees complied with all applicable state laws pertaining to the protection and confidentiality of Plaintiff's and Class Members' Private Information.

271. Plaintiffs' and Class Members' Private Information was accessed in an unauthorized manner while in the custody of Defendant.

272. Plaintiffs' and Class Members' Private Information was accessed by and/or distributed to one or more unauthorized third parties while in the custody of Defendant.

273. Defendant did not adequately protect Plaintiffs' and Class Members' Private Information, nor did it detect and/or prevent unauthorized access to Plaintiff's and Class Members' Private Information.

274. Defendant's failure to protect Plaintiffs' and Class Member's Private Information led to an unreasonable, substantial, and serious interference of Plaintiffs' and Class Members' privacy.

275. The acts and omissions of Defendant described above constitute a violation of MASS. GEN. LAWS ch. 214, §1B.

276. As a direct and proximate result of Defendant's deceptive acts or practices, Plaintiffs and the Class have suffered and will continue to suffer injury, ascertainable losses of

money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have sought medical services from Defendant but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Private Information; and an increased, imminent risk of fraud and identity theft.

277. Defendant's violations present a continuing risk to Plaintiffs Smith, and Class Members as well as to the general public.

278. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive damages, and attorneys' fees and costs.

PRAYER FOR RELIEF

A. That the Court certify this action as a class action and certify the Class as proper and maintainable pursuant to Rule 23 of the Massachusetts Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Counsel as Class counsel;

B. That the Court grant permanent injunctive relief to prohibit Shields from engaging in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and members of the Class compensatory, consequential, and general damages in an amount to be determined at trial;

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

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

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

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

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

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

Dated: January 9, 2023

Respectfully submitted,

BERMAN TABACCO

/s/ Nathaniel L. Orenstein
Nathaniel L. Orenstein (BBO #664513)
Patrick T. Egan (BBO #637477)
Christina L. Gregg (BBO #709220)
One Liberty Square
Boston, MA 02109
Telephone: (617) 542-8300
pegan@bermantabacco.com
norenstein@bermantabacco.com
cgregg@bermantabacco.com

Jason M. Leviton (BBO #678331)
Brendan Jarboe (BBO #691414)
BLOCK & LEVITON LLP
260 Franklin Street, Suite 1860
Boston, MA 02110
Telephone: (617) 398-5600
Facsimile: (617) 507-6020
jason@blockleviton.com
brendan@blockleviton.com

Interim Co-Liaison Counsel

Lori G. Feldman, Esq.
GEORGE GESTEN MCDONALD, PLLC
102 Half Moon Bay Drive
Croton-on-Hudson, NY 10520

Telephone: (561) 232-6002
Facsimile: (888) 421-4173
lfeldman@4-justice.com
E-Service: eService@4-justice.com

Seth A. Meyer
KELLER POSTMAN LLC
150 N. Riverside Plaza, Suite 4100
Chicago, IL 60606
Telephone: (312) 741-5220
sam@kellerpostman.com

Elizabeth Pollock-Avery
Gary F. Lynch
Hannah N. Barnett
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
elizabeth@lcllp.com
hannah@lcllp.com

Interim Co-Lead Counsel

Stephen R. Basser
BARRACK, RODOS & BACINE
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874
sbasser@barrack.com

Melissa R. Emert
Gary S. Graifman
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
135 Chestnut Ridge Road
Suite 200
Montvale, NJ 07645
Telephone: (201) 391-7000
Facsimile: (201) 307-1086
memert@kgglaw.com
ggraifman@kgglaw.com

Todd. S. Garber
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, NY 10601
Telephone: (914) 298-3281
Facsimile: (914) 824-1561
tgarber@fbfglaw.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 Monroe Street, Suite 2100
Chicago, IL 60606
gklinger@milberg.com

Kenya J. Reddy
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
kreddy@ForThePeople.com

Carey Alexander
Erin Green Comite
SCOTT+SCOTT, ATTORNEYS AT LAW, LLP
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
calexander@scott-scott.com
ecomite@scott-scott.com

Victoria Santoro Mair
SWEENEY MERRIGAN LAW, LLP
268 Summer Street, LL Boston, MA 02210
Telephone: (617) 391-9001
Facsimile: (617) 357-9001
victoria@sweeneymerrigan.com

Carl V. Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC

111 W. Jackson Blvd., Suite 1700
Chicago, IL 60604
Telephone: (312) 984-0000
Facsimile: (212) 686-0114
malmstrom@whafh.com

Interim Executive Committee

CERTIFICATE OF SERVICE

I hereby certify that on January 9, 2023, a copy of the foregoing was filed electronically. Service of this filing will be made on all ECF-registered counsel by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/ Nathaniel L. Orenstein
Nathaniel L. Orenstein