UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

In re Shields Healthcare Group, Inc. Data Breach Litigation	**Civil Action No.: 1:22-cv-10901-PBS** **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs James Buechler, Julie Colby, John Kennedy, Sharon Pimental, and Cindy Tapper (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, allege as, and for their Consolidated Class Action Complaint, the following against Shields Health Care Group Inc. ("Shields" or "Defendant"). The following allegations are based upon Plaintiffs' personal knowledge with respect to themselves and their own acts, and following their investigation and the investigation of their counsel, and upon information and belief as to all other matters.

I. INTRODUCTION

1. Shields provides MRI, PET/CT, and ambulatory surgical services to patients at more than forty 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 the New England region, including Massachusetts, Maine, Maryland, Rhode Island, and New Hampshire. Shields also provided healthcare services during this time to patients in additional neighboring states who traveled to Shields facilities from their home state to receive healthcare services from Defendant and thereafter moved to other states. Moreover, Shields reported sending notice of the data breach to patients who reside in, among others, the following additional states (as publicly reported on the data breach reporting websites of the following U.S. Attorneys' General): Texas, Vermont, Washington, Indiana, California, Oregon, and Montana.

2. This class action is brought on behalf of citizens of all states in the United States, including but not limited to Maine, Maryland, Rhode Island, and New Hampshire – with the exception of and excluding citizens of Massachusetts – who are the victims of a targeted, intentional cyber-attack at Defendant's medical facilities that allowed third party criminal hackers to access Defendant's computer systems and exfiltrate patient data from approximately March 7, 2022 to March 21, 2022 (the "Class" and "Class Members"), 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 Class Members within 60 days as required by law. 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."[2]

---

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

[2] 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.

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.

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 HIPAA, and other Private Information.[3]

8. Plaintiffs bring this class action lawsuit on behalf of themselves and all others 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.

---

[3] 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).

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 risk for improper disclosure of Plaintiffs' and Class Members' Private Information were known and foreseeable to Defendant. Thus, Defendant was on notice that failing to take steps necessary 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 a heightened risk of exposure 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 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 identify 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.

18. 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.

19. 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.

20. 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, breach of implied covenant of good faith and fair dealing, negligent misrepresentation, invasion of privacy by intrusion, breach of fiduciary duty, breach of confidence, declaratory judgment, unjust enrichment, violation of the Rhode Island Deceptive Trade Practices Act, R.I. GEN. LAWS §§6-13.1-1, *et seq.*, violation of the Maine Unfair Trade Practices Act, ME. STAT. tit. 5, §§205, 213, *et seq.*, violation of the Maine Uniform Deceptive Trade Practices Act, ME. STAT. tit. 10, §§1212, *et seq.*, violation of the Maine Confidentiality of Health Care Information Law, ME. STAT. tit. 22, §1711-C, violation of the Maryland Consumer Protection Act, MD. CODE, COM. LAW §§13-101, *et seq.*, violation of the Maryland Personal Information Protection Act, MD. CODE, COM. LAW, §§14-3501, *et seq.*, violation of the Maryland Social Security Number Privacy Act, MD. CODE, COM. LAW, §§14-3401, *et seq.*, violation of the New Hampshire Consumer Protection Act, N.H. REV. STAT. §§358-A, *et seq.*, and violation of the New Hampshire Notice of Security Breach statute, N.H. REV. STAT. Ann. §§359-C:20, *et seq*, violation of the Massachusetts Consumer Protection Act, MASS. GEN. LAWS ch. 93A, §§1, *et seq*.

II. PARTIES

21. Plaintiff James Buechler ("Plaintiff Buechler") is a resident of Baltimore County, Maryland and a citizen of Maryland. Plaintiff Buechler was a Shields patient at all times relevant to the Data Breach. Mr. Buechler learned of the Shields Data Breach through a notice posted on Shields' website that his Private Information was improperly exposed to unauthorized third parties.

22. Plaintiff Julie Colby ("Plaintiff Colby") is a resident of Androscoggin County, Maine and a citizen of Maine. Plaintiff Colby was a Shields patient at all times relevant to the

Data Breach. She received letter notice from Shields that her Private Information was improperly exposed to unauthorized third parties.

23. Plaintiff John Kennedy ("Plaintiff Kennedy") is a resident of Kent County, Rhode Island and a citizen of Rhode Island. He received letter notice from Shields that his Private Information was improperly exposed to unauthorized third parties.

24. Plaintiff Sharon Pimental ("Plaintiff Pimental") is a resident of Newport County, Rhode Island and a citizen of Rhode Island. Plaintiff Pimental was a Shields patient at all times relevant to the Data Breach. She received letter notice from Shields that her Private Information was improperly exposed to unauthorized third parties.

25. Plaintiff Cindy Tapper ("Plaintiff Tapper") is a resident of Strafford County, New Hampshire and a citizen of New Hampshire. Plaintiff Tapper was a Shields patient at all times relevant to the Data Breach. She received letter notice from Shields that her Private Information was improperly exposed to unauthorized third parties.

26. Defendant Shields is a Massachusetts corporation with its principal place of business in Quincy, Massachusetts. Shields is a provider of health care that has more than 40 facilities throughout New England, as well as in Maine, Maryland, Rhode Island, and New Hampshire, offering MRI, PET/CT, and outpatient surgical services. Shields also provided healthcare services during this time to patients in additional neighboring states who traveled to Shields facilities from their home state to receive healthcare services from Defendant. Moreover, Shields reported sending notice of the data breach to patients who reside in the following additional states (as publicly reported on the data breach reporting websites of the following U.S. Attorneys' General): Texas, Vermont, Washington, Indiana, California, Oregon, and Montana.

III. JURISDICTION AND VENUE

27. This Court has subject-matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. §1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and there are thousands of members of the class that are citizens of states different from Defendant.

28. This Court has personal jurisdiction over Defendant because Shields is headquartered in Massachusetts, its principal place of business is in Massachusetts, and it regularly conducts business in Massachusetts.

29. Venue is proper in this Court pursuant to 28 U.S.C. §1391 because a Defendant resides in this District, a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this District, Shields is based in this District, Shields maintains patients' Private Information in the District, and Defendant has caused harm to Plaintiffs and Class Members residing in this District.

IV. STATEMENT OF FACTS

A. Shields' Business

30. 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.

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

32. Patients demand security to safeguard their Private Information. As a healthcare provider, Shields is required to ensure that such Private Information is not disclosed or disseminated to unauthorized third parties without the patients' express written consent, as further detailed below.

B. The Data Breach

33. Beginning on or around March 7, 2022 through March 21, 2022, unauthorized third-party computer hackers accessed Shields' computer system 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.

34. After learning of the Data Breach, Shields commenced an investigation. That investigation revealed that approximately two million patients 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.

35. 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:

> [F]ull 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. (the "Notice").[4]

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

36. 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, 2022. The Notice indicated that the "suspicious activity may have involved data compromise" and that Shields "immediately launched an investigation into this issue. "[5]

37. 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.[6]

38. It took Shields nearly three months after the Data Breach to inform Plaintiffs 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.

39. Shields' Notice 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

---

5 *Id.*

6 *Id.*

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.

40. 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, unredacted Private 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

James Buechler

41. Plaintiff James Buechler has been a patient of Shields for years. Mr. Buechler and his wife were patients of Mercy Hospital, which contains a Shields imaging facility where they both underwent various imaging.

42. On multiple occasions, Plaintiff Buechler has been required to provide his Private Information to Shields as a condition of his treatment. Plaintiff Buechler specifically recalls providing Shields with his driver's license, credit card, Social Security number, and photograph when he visited Mercy Hospital for imaging.

43. Plaintiff received a Notice of the Security Incident (the "Data Breach Notice"), sent by Defendant.

44. After receiving the Data Breach Notice, Plaintiff Buechler spent at least 10 to 15 hours dealing with the consequences of the Data Breach and continues to spend many hours dealing 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 thousands of dollars of fraudulent charges to his Bank of America account, purchasing identity protection, and dealing with suspicious activity found in his AOL email account, all as a result of his Private Information being exposed in the Data Breach. Plaintiff Buechler intends to spend additional time and effort taking steps to protect his Private Information in the future. Because of the Data Breach, Plaintiff Buechler spent valuable time he otherwise would have spent on other obligations.

45. Moreover, Plaintiff Buechler spent this time at Shields' direction. In the Data Breach Notice Plaintiff Buechler 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."

46. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Buechler 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.

47. After the Data Breach, Plaintiff Buechler experienced identity fraud in the form of thousands of dollars of unauthorized charges on his Bank of America card. As a result, Mr. Buechler was without his payment card, which had a 3% cash back discount, for three days and was forced to use his Bank of America business payment card, which had a lower percentage cash back discount. This also caused him to have bookkeeping issues as he had to repay his business for the personal charges and accurately account for them. In addition, Plaintiff Buechler had to disable and re-link the automatic payments on the account to ensure future payments were paid on time.

48. In April 2022, shortly after the Data Breach, Mr. Buechler was contacted by AOL about fraudulent activity found within his email account, which caused AOL to freeze his account. The email account is, and has been for many years, his primary email account. The account contained highly sensitive financial account information, which further increased Plaintiff Buechler's concerns. Plaintiff Buechler spent many hours corresponding with AOL in order to regain access to his account.

49. As a result of the Data Breach, Plaintiff Buechler purchased identity theft protection through AllClear for $299 per year.

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

51. In addition, Plaintiff Buechler 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 and the release of his protected health information, which he would not have suffered had Defendant Shields implemented the necessary and proper safeguards to protect its patients' Private Information from theft.

52. 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 foreseeable that Plaintiff Buechler would take, and continue to take, necessary measures to protect his Private Information.

53. Plaintiff Buechler 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.

54. Plaintiff Buechler suffered actual injury in the form of fraudulent charges to his Bank of America card, lost benefits and discounts associated with his Bank of America card, and time spent on bookkeeping issues as he had to repay his business for the personal charges and accurately account for them. He also purchased identity theft protection, which costs him $299 per year. In addition, Plaintiff Buechler 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 Buechler has also suffered actual injury in the form of lost time by having to deal with all 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 thousands of dollars of fraudulent charges to his Bank of America account, purchasing identity protection, and dealing with suspicious activity found in his AOL account, all as a result of his Private Information being exposed in the Data Breach.

Julie Colby

55. Plaintiff Colby has been regularly using Shields imaging, located in Topsham, Maine for her annual mammograms for years. On December 15, 2021, Plaintiff Colby went to Shields for a chest x-ray.

56. Plaintiff Colby's Private Information was available to Shields through either her doctor's office, and/or Central Maine Healthcare, with which her doctor is associated, and which provided her Private Information to Shields.

57. Plaintiff Colby received a Data Breach Notice informing her of the Data Breach sometime in June 2022.

58. Thereafter, Plaintiff Colby spent time taking action to mitigate the impact of the Data Breach after she received the Data Breach Notice, which included diligently checking her accounts and her financial accounts. This is time Plaintiff Colby otherwise would have spent performing other activities or leisurely events for the enjoyment of life.

59. After the Data Breach, Plaintiff Colby was subject to a potential fraud concerning her health insurance. Specifically, after the Data Breach, Plaintiff received two calls, one during the evening of June 28, 2022, and another during the evening of July 8, 2022, in which the caller was attempting to reach her to purportedly speak to her about her health insurance plan. Both calls were from the same phone number. Upon receiving these calls, Plaintiff Colby researched the telephone number on the internet and determined that the calls were made from a scammer who likely had access to information about her health insurance plan.

60. Since the Data Breach, Plaintiff Colby has further received an increase in spam telephone calls.

61. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of her protected health information which she expected Shields to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing, and potentially using his Private Information.

62. Plaintiff Colby suffered actual injury from having her Private Information exposed as a result of the Data Breach including, but not limited to: (a) paying monies to Shields for its goods and services which she would not have paid had Shields disclosed that it lacked data security practices adequate to safeguard patients' Private Information from theft; (b) damages to and diminution in the value of her Private Information – a form of intangible property that Plaintiff entrusted to Shields as a condition for healthcare services; (c) loss of her privacy; and (d) imminent and impending injury arising from the increased risk of fraud and identity theft.

63. As a result of the Data Breach, Plaintiff Colby will continue to be at heightened risk for financial fraud, medical fraud and identity theft, and the attendant damages, for years to come.

John Kennedy

64. Plaintiff Kennedy received letter notice from Shields that his Private Information was improperly exposed to unauthorized third parties.

65. Although Shields discovered the Data Breach on March 28, 2022, Plaintiff Kennedy was not notified of the Data Breach until sometime after July 22, 2022.

66. According to the Notice of Security Incident dated July 22, 2022 (the "Data Breach Notice"), sent by Defendant Shields to Plaintiff Kennedy, Plaintiff Kennedy's personal information, which included full name, home address, telephone number, and social security number was exposed in the Data Breach, and Defendant Shields learned of same on March 28, 2022.

67. After receiving the Data Breach Notice, Plaintiff Kennedy spent at least 10 hours dealing with the consequences of the Data Breach and continues to spend many hours dealing with the consequences of the Data Breach, including reviewing and monitoring his bank accounts, credit card accounts, credit reports and other online accounts, reviewing dark web alerts, researching the

potential impact of the Data Breach, as a result of his Private Information being exposed in the Data Breach. Plaintiff Kennedy intends to spend additional time and effort taking steps to protect his Private Information in the future. Because of the Data Breach, Plaintiff Kennedy spent valuable time he otherwise would have spent on other obligations.

68. Moreover, Plaintiff Kennedy spent this time at Shields' direction. In the notice letter Plaintiff Kennedy 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."

69. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Kennedy 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.

70. Plaintiff Kennedy's increased concerns are further enhanced by recent "phishing" correspondence that he received after receiving the Data Breach Notice, including receiving several calls each day. Although he tries to block the calls, they continue to call from different numbers.

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

72. In addition, Plaintiff Kennedy 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 Information from theft.

73. 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 foreseeable that Plaintiff Kennedy would take, and continue to take, necessary measures to protect his Private Information.

74. Plaintiff Kennedy 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.

75. Plaintiff 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. In addition, Plaintiff Kennedy has 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, credit reports and other online accounts, researching the potential impact of the Data Breach, evaluating freezing his credit with credit reporting agencies and credit protection services, and dealing with an increase in spam calls, all as a result of the Data Breach.

Sharon Pimental

76. Plaintiff Pimental has been a patient of Shields for approximately three years.

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

78. Although Shields discovered the Data Breach on March 28, 2022, Plaintiff Pimental did not receive a Data Breach Notice until sometime after June/July of 2022.

79. According to the Data Breach Notice sent by Defendant to Plaintiff Pimental, Plaintiff Pimental's personal information was exposed in the Data Breach, and Defendant learned of same on March 28, 2022.

80. After receiving the Data Breach Notice, Plaintiff Pimental spent time dealing with the consequences of the Data Breach and continues to spend time dealing with the consequences of 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 evaluating freezing her credit with credit reporting agencies and credit protection services, all as a result of her Private Information being exposed in the Data Breach. Plaintiff Pimental intends to spend additional time and effort taking steps to protect her Private Information in the future. Because of the Data Breach, Plaintiff Pimental spent valuable time she otherwise would have spent on other obligations.

81. Moreover, Plaintiff Pimental spent this time at Shields' direction. In the Data Breach Notice Plaintiff Pimental 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."

82. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Pimental 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.

83. Plaintiff Pimental's increased concerns are further enhanced by recent "phishing" correspondence that she received after receiving the Data Breach Notice, including calls regarding solicitation from medical companies for medical equipment and devices.

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

85. In addition, Plaintiff Pimental 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 implemented the necessary and proper safeguards to protect its patients' Private Information from theft.

86. 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 foreseeable that Plaintiff Pimental would take, and continue to take, necessary measures to protect her Private Information.

87. Plaintiff Pimental 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.

88. Plaintiff 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. In addition, Plaintiff Pimental has suffered actual injury in the form of lost time by having to deal with the consequences of 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, evaluating freezing her credit with credit reporting agencies and credit protection services, and dealing with an increase in spam calls, all as a result of the Data Breach.

Cindy Tapper

89. Plaintiff Tapper has been a patient of Shields for approximately one year.

90. Plaintiff Tapper has been required to provide her Private Information to Shields as a condition of her treatment.

91. Although Shields discovered the Data Breach on March 28, 2022, Plaintiff Tapper did not receive a Data Breach Notice until sometime after July 26, 2022.

92. According to the Notice of Security Incident dated July 26, 2022 (the "Data Breach Notice"), sent by Defendant to Plaintiff Tapper, Plaintiff Tapper's personal information, which included full name, home address, telephone number, date of birth, patient ID number, medical record number, and other medical or treatment information, was exposed in the Data Breach, and Defendant learned of same on March 28, 2022.

93. After receiving the Data Breach Notice, Plaintiff Tapper spent approximately five hours dealing with the consequences of the Data Breach and continues to spend many hours dealing with the consequences of 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 evaluating freezing her credit with credit reporting agencies and credit protection services, all as a result of her Private Information being exposed in the Data Breach. Plaintiff Tapper intends to spend additional time and effort taking steps to protect her Private Information in the future. Because of the Data Breach, Plaintiff Tapper spent valuable time she otherwise would have spent on other obligations.

94. Moreover, Plaintiff Tapper spent this time at Shields' direction. In the Data Breach Notice Plaintiff Tapper 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."

95. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Tapper 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.

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

97. In addition, Plaintiff Tapper 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 implemented the necessary and proper safeguards to protect its patients' Private Information from theft.

98. 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 Tapper would take, and continue to take, necessary measures to protect her Private Information.

99. Plaintiff Tapper 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.

100. Plaintiff 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. In addition, Plaintiff Tapper has suffered actual injury in the form of lost time by having to deal with the consequences of 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, evaluating freezing her credit with credit reporting agencies and credit protection services, and dealing with an increase in spam calls, all as a result of the Data Breach.

D. Shields' Privacy Policies

101. 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."

102. 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.

103. 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

104. Defendant was specifically on notice that the Federal Bureau of Investigation ("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).'"7

105. 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 of patients' health and financial information, but also patient access to care.[8]

106. 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.9 In 2017, a new record high of 1,579 breaches were reported representing a 44.7% increase.10 That upward trend continues.

---

7 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.

8 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 (emphasis omitted).

9 *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.

10 *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).

107. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.11 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.12 Almost 50% of the victims lost their healthcare coverage as a result of the incident, while nearly thirty percent said their insurance premiums went up after the event. Forty percent of the customers were never able to 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.13

108. 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.14

> Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information (PII) for thousands of patients at any given time. From social security and insurance policies to next of kin and credit

---

11 *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).

12 Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

13 *Id.*

14 *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).

> cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.[15]

109. As a healthcare provider, Shields knew, or reasonably 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. The consequences include 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.

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

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

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

112. 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 Plaintiffs' and Class Members' Private Information from disclosure.

113. Plaintiffs 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.

---

[15] 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. The Value of Private Information and the Effects of Unauthorized Disclosure

114. 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.

115. Private Information is a valuable commodity to identity thieves. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.16 Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

116. 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.17

117. 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.

118. Medical identify 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

---

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

17 *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).

financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities.'"18

119. 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 difficult to detect, taking almost twice as long as normal identity theft.[19]

120. 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.

121. 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.

122. 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. 40% of consumers found out they were a victim of medical

---

18 Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

19 *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIV. (Apr. 8, 2014), https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf.

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

identity theft only when they received collection letters from creditors for expenses that were incurred in their names.21

123. As a healthcare provider, Shields knew, or reasonably 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.

G. Shields' Conduct Violates HIPAA

124. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.22

125. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

---

21 *The Potential Damages and Consequences of Medical Identify 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.

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/.

126. The HIPAA Breach Notification Rule, 45 CFR §§164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of a breach."23

127. Based on information and belief, Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. Shields' security failures include, but are not limited to, the following:

i. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

ii. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

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

iv. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

v. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

vi. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

vii. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(94);

---

[23] *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Jan. 6, 2023) (emphasis added).

viii. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

ix. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

x. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

H. Shields Failed to Comply with FTC Guidelines

128. Shields was also prohibited by the Federal Trade Commission Act ("FTCA") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA. See, e.g., FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

129. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.24

130. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.25 The guidelines note that businesses should protect the personal customer information that they keep; properly dispose

---

[24] *Start With Security: A Guide for Business*, FED. TRADE COMM'N, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 6, 2023).

[25] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION,available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 6, 2023).

of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

131. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.26

132. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. §45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

133. Shields failed to properly implement basic data security practices. Shields' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. §45.

134. Shields was at all times fully aware of its obligation to protect the Private Information of patients because of its position as a trusted healthcare provider. Shields was also aware of the significant repercussions that would result from its failure to do so.

---

26 *See* n.24, *supra*.

I. Shields Failed to Comply with Healthcare Industry Standards

135. 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 sensitive and valuable data.[27]

136. 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.

137. 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.[28] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

138. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Shields chose to ignore them. These best practices were

---

[27] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA J. (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/.

[28] *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.

known, or reasonably 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.

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

139. 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.

140. Every year, identity theft causes tens of billions of dollars of losses to victims in the United States.[29] 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.[30] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

---

[29] *Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited on Jan. 6, 2023) (discussing Javelin Strategy & Research's report *2018 Identity Fraud: Fraud Enters a New Era of Complexity*).

[30] *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/.

141. 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.

142. 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.[31]

143. 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.[32]

144. 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 other crimes, and steal benefits.[33]

145. 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 have exposed the Plaintiffs and Class Members.

---

[31] 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-will-identity-thieves-use-stolen-info [http://web.archive.org/web/20220201130728/https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info].

[32] 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 [https://wayback.archive-it.org/all/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html].

[33] *See, e.g.*, *supra* note 30.

K. Plaintiffs and Class Members Suffered Damages

146. 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.[34]

147. 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.

148. 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.

149. 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 risk of identity theft and fraud.

150. 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

[34] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be 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.

151. 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.

152. Plaintiffs and Class Members did not receive the full benefit of the bargain for received healthcare and other services. Instead, these services were of a diminished value to that described in their agreements with Shields. As a result, Plaintiffs 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 without the data security protection.

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

154. 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.

155. 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.

156. 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.

157. 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.

158. 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.

159. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "[r]esolving the problems caused by identity theft [could] take more than a year for some victims."[35]

160. 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 sits by and does nothing to assist those affected by the

[35] 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.

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.

161. 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 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.

162. 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.

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

163. 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.[36]

164. 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 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 it wasn't reported, they can't take action to protect themselves. . . . ".[37]

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

166. 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

167. Plaintiffs brings this class action on behalf of themselves herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

168. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **Nationwide Class: All individuals whose Private Information was compromised in the data breach of Shields' systems from approximately**

---

[36] *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.

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

March 7, 2022 to March 21, 2022. Excluded from the Nationwide Class are citizens of Massachusetts.

169. In the alternative to the Nationwide Class, Plaintiffs seek certification of the following state Sub-Classes:

> **Maryland Sub-Class: All citizens of Maryland whose Private Information was compromised in the data breach of Shields' systems from approximately March 7, 2022 to March 21, 2022.**
>
> **Maine Sub-Class: All citizens of Maine whose Private Information was compromised in the data breach of Shields' systems from approximately March 7, 2022 to March 21, 2022.**
>
> **Rhode Island Sub-Class: All citizens of Rhode Island whose Private Information was compromised in the data breach of Shields' systems from approximately March 7, 2022 to March 21, 2022.**
>
> **New Hampshire Sub-Class: All citizens of New Hampshire whose Private Information was compromised in the data breach of Shields' systems from approximately March 7, 2022 to March 21, 2022.**

170. The Nationwide Class and Maryland, Maine, Rhode Island, and New Hampshire Sub-classes are together referred to as the "Classes." Excluded from the Classes are: All citizens of Massachusetts. Also excluded from the Classes 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.

171. Plaintiff reserves the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

172. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of all members is impracticable. Defendant has identified more than 1.8 million patients whose Private Information may have been improperly accessed in the Data Breach whose Private Information was compromised, and the Classes are apparently identifiable within Defendant's records.

173. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes 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 Classes 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' Private Information;

vi. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' Private Information 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 Classes 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.

174. Typicality, Fed. 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.

175. 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 Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Classes and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Classes uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

176. Adequacy, Fed. 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 Classes 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.

177. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): 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.

178. The nature of this action and the nature of laws available to Plaintiffs and the Classes make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Classes 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 of the individual Classes 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 Classes 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.

179. 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.

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

181. 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

Classes 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.

182. Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Classes as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

i. Whether Defendant owed a legal duty to Plaintiffs and Classes 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 Nationwide Class)

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

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

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

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

188. 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.

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

190. 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 – information that Plaintiffs and the Class Members had been required to provide to Shields.

191. 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.

192. 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 reasonably should have known it was failing to meet its duties, and that Defendant's breach of such duties would cause

Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

193. 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 Nationwide Class)

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

195. Pursuant to the FTCA (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.

196. 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.

197. Defendant breached its duties to Plaintiffs and Class Members under the FTCA (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.

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

199. 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.

200. 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 reasonably 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.

201. 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 Nationwide Class)

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

203. 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.

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

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

206. 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 Nationwide Class)

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

208. 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' privacy duties and policies.

209. 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 Private Information was breached or otherwise compromised.

210. 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.

211. 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 involving Private Information was critical to realize the intent of the parties.

212. 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 Data Breach.

213. As a direct and proximate result of Shields' 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 Nationwide Class)

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

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

216. 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.

217. 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.

218. 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.

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

220. Shields' 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.

221. Shields' 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.

222. Accordingly, Plaintiffs and Class Members have been injured as a result of Shields' 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 Nationwide Class)

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

224. 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.

225. 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.

226. 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.

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

228. 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.

229. 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 Nationwide Class)

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

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

232. 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.

233. 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 Private Information 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.

234. 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.

235. 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.

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

237. Shields' 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.

238. 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.

239. Plaintiffs and Class Members had a reasonable expectation of 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.

240. 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.

241. As a 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 Nationwide Class)

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

243. 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.

244. 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.

245. 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, and in particular, to keep secure the Private Information of those patients.

246. 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. §64.308(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.

247. 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 the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (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 Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

248. 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 Nationwide Class)

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

250. 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.

251. 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.

252. 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.

253. 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.

254. 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.

255. 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.

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

257. 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.

258. 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 storing 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.

259. 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 to decide 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 of exposure 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.

260. 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 Nationwide Class)

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

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

263. 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' 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 Private Information will occur in the future.

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

265. Shields owes a legal duty to secure patients' Private Information and to timely notify patients of a data breach under the common law, §5 of the FTCA and HIPAA.

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

267. 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.

268. 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.

269. The hardship to Plaintiffs and Class Members if an injunction is not issued 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.

270. 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 Nationwide Class)

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

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

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

274. 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.

275. 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.

276. Under principles 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.

277. 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.

278. 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 Rhode Island Deceptive Trade Practices Act, R.I. GEN. LAWS §§6-13.1-1, *et seq*.

(On Behalf of Plaintiffs Kennedy and Pimental and the Rhode Island Sub-Class)

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

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

281. Defendant is engaged in the advertising, offering for sale, sale, or distribution of any services and any property, tangible or intangible, real, personal, or mixed, and any other article, commodity, or thing of value wherever situated, and include any trade or commerce directly or indirectly affecting the people of the state of Rhode Island.

282. Defendant has engaged in unfair methods of competition and unfair or deceptive acts or practices.

283. Defendant has represented that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have.

284. Defendant has represented that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, when they are of another.

285. Defendant has engaged in conduct that creates a likelihood of confusion or of misunderstanding.

286. Defendant has engaged in acts or practices that are unfair or deceptive to its consumers.

287. Defendants has used methods, acts, or practices that mislead or deceive members of the public in a material respect.

288. Defendant misrepresented that it would keep the Private Information of Plaintiffs Kennedy and Pimental and Rhode Island Sub-Class Members secure, private, and confidential.

289. Defendant had a duty to keep the Private Information safe and secure under HIPAA and regulations promulgated thereunder, and the FTCA and regulations promulgated thereunder.

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

291. Defendant failed to comply with its obligations to protect and secure the Private Information under HIPAA and regulations promulgated thereunder, and the FTCA and regulations promulgated thereunder.

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

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

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

295. Defendant had a duty to timely notify patients, including Plaintiffs Kennedy and Pimental and the members of the Rhode Island Sub-Class Members, of the Data Breach under 45 C.F.R. §164.404.

296. Although it was aware of the Data Breach, Defendant failed to timely notify its patients of the Data Breach, including Plaintiffs Kennedy and Pimental and the members of the Rhode Island Sub-Class.

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

298. As a result of the aforementioned actions and omissions, Plaintiffs Kennedy and Pimental and the Rhode Island Sub-Class Members 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.

299. As a result of the aforementioned actions and omissions, Plaintiffs Kennedy and Pimental and the Rhode Island Sub-Class Members seek their actual damages, statutory damages, treble damages, punitive damages, restitution 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.

COUNT XIII
Violation of the Maine Unfair Trade Practices Act, ME. STAT. tit. 5, §§205, 213, *et seq*.
(On Behalf of Plaintiff Colby and the Maine Sub-Class)

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

301. Defendant is a "person" as defined by ME. STAT. tit. 5, §206(2).

302. Defendant's conduct as alleged herein related was in the course of "trade and commerce" as defined by ME. STAT. tit. 5, §206(3).

303. Plaintiff Colby and Maine Sub-Class Members purchased goods and/or services for personal, family, and/or household purposes.

304. Shields engaged in unfair and deceptive trade acts and practices in the conduct of trade or commerce, in violation of ME. STAT. tit. 5, §207, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Colby and Maine Sub-Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Colby and Maine Sub-Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. §45, HIPAA, 42 U.S.C. §1320d, and Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§6501-6505, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Colby and Maine Sub-Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Colby and Maine Sub-Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. §45, HIPAA, 42 U.S.C. §1320d, and COPPA, 15 U.S.C. §§6501-6505;

f. Failing to timely and adequately notify Plaintiff Colby and Maine Sub-Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Colby and Maine Sub-Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Colby and Maine Sub-Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. §45, HIPAA, 42 U.S.C. §1320d, and COPPA, 15 U.S.C. §§6501-6505.

305. Shields' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Shields' data security and ability to protect the confidentiality of consumers' Private Information.

306. Shields' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff Colby and Maine Sub-Class Members, that their Private Information was not exposed, and misled Plaintiff Colby and Maine Sub-Class Members into believing they did not need to take actions to secure their identities.

307. Had Shields disclosed to Plaintiff Colby and Maine Sub-Class Members that its data systems were not secure and, thus, vulnerable to attack, Shields would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law and industry standards. Instead, Shields was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff, the Class, and the Maine Sub-Class. Shields accepted the responsibility of being a steward of this data while

keeping the inadequate state of its security controls secret from the public. Accordingly, because Shields held itself out as maintaining a secure platform for Private Information data, Plaintiff, the Class, and the Maine Sub-Class Members acted reasonably in relying on Shields' misrepresentations and omissions, the truth of which they could not have discovered.

308. As a direct and proximate result of Defendant's unfair and deceptive acts and conduct, Plaintiff Colby and Maine Sub-Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

309. Plaintiff Colby and Maine Sub-Class Members seek non-monetary relief allowed by law, including damages or restitution, injunctive and other equitable relief, and attorneys' fees and costs.

310. Plaintiff sent a demand for relief on behalf of the Maine Subclass pursuant to 5 Me. Rev. Stat. §213(1-A).

COUNT XIV
Violation of the Maine Uniform Deceptive Trade Practices Act, ME. STAT. tit. 10, §§1212, *et seq*.
(On Behalf of Plaintiff Colby and the Maine Sub-Class)

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

312. Defendant is a "person" as defined by ME. STAT. tit. 10, §1211(5).

313. Shields advertised, offered, or sold goods or services in Maine and engaged in trade or commerce directly or indirectly affecting the people of Maine.

314. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of ME. STAT. tit. 10, §1212.

315. Defendant's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Colby and Maine Sub-Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Colby and Maine Sub-Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. §45, HIPAA, 42 U.S.C. §1320d, and COPPA, 15 U.S.C. §§6501-6505, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Colby and Maine Sub-Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Colby and Maine Sub-Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. §45, HIPAA, 42 U.S.C. §1320d, and COPPA, 15 U.S.C. §§6501-6505;

f. Failing to timely and adequately notify Plaintiff Colby and Maine Sub-Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Colby and Maine Sub-Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Colby and Maine Sub-Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. §45, HIPAA, 42 U.S.C. §1320d, and COPPA, 15 U.S.C. §§6501-6505.

316. Shields' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Shields' data security and ability to protect the confidentiality of consumers' Private Information.

317. Shields' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff Colby and Maine Sub-Class Members, that their Private Information was not exposed, and misled Plaintiff Colby and Maine Sub-Class Members into believing they did not need to take actions to secure their identities.

318. Shields intended to mislead Plaintiff Colby and Maine Sub-Class Members and induce them to rely on its misrepresentations and omissions.

319. Had Shields disclosed to Plaintiff Colby and Maine Sub-Class Members that its data systems were not secure and, thus, vulnerable to attack, Shields would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and that comply with the law and industry standards. Instead, Shields was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff Colby and the Maine Sub-Class. Shields Health accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Shields held itself out as maintaining a secure platform for Private Information data, Plaintiff Colby and Maine Sub-Class Members acted reasonably in relying on Shields' misrepresentations and omissions, the truth of which they could not have discovered.

320. As a direct and proximate result of Shields' deceptive trade practices, Plaintiff Colby and Maine Sub-Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

321. Maine Sub-Class Members are likely to be damaged by Defendant's ongoing deceptive trade practices.

322. Plaintiff Colby and Maine Sub-Class Members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive or other equitable relief, and attorneys' fees and costs.

COUNT XV
Violation of the Maine Confidentiality of Health Care Information Law, ME. STAT. tit. 22, §1711-C
(On Behalf of Plaintiff Colby and the Maine Sub-Class)

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

324. The Maine Confidentiality of Health Care Information law prohibits, among other things, unauthorized disclosure of patient health care records. ME. STAT. tit. 22, §1711-C (2).

325. Plaintiff Colby provided PHI to Shields which is a "health care practitioner" as defined by ME. STAT. tit. 22, §1711-C (1)(F).

326. Shields is a "health care practitioner" as defined by ME. STAT. tit. 22, §1711-C (1)(F).

327. Plaintiff Colby is an "individual" whose health care information was disclosed without proper authorization as defined by ME. STAT. tit. 22, §1711-C (1)(G).234. Shields had a duty to develop and implement policies, standards and procedures to protect the confidentiality, security and integrity of the Plaintiff Colby and Maine Sub-Class Members' health care information to ensure that information is not negligently, inappropriately or unlawfully disclosed. ME. STAT. tit. 22, §1711-C (7). 235. Shields disclosed health care information pertaining to the Plaintiff Colby and Maine Sub-Class without their consent and for no other reason permitted by ME. STAT. tit. 22, §1711-C.

328. Unauthorized disclosure of health care information to hackers resulted from the affirmative actions of Shields in maintaining the security of its computer system at levels that did not protect the confidentiality, security and integrity of Plaintiff Colby and Maine Sub-Class Members' health care information and allowed hackers to improperly access and copy private health care information of the Plaintiff Colby and Maine Sub-Class.

329. The affirmative actions of Shields in maintaining the security of its computer system at levels allowed hackers to improperly access and copy private health care information of the Plaintiff Colby and Maine Sub-Class. Shields actively and affirmatively allowed the hackers to see and obtain the health care information of the Plaintiff Colby and Maine Sub-Class Members.

330. Plaintiff Colby and Maine Sub-Class Members were injured and have suffered damages from Shields' illegal disclosure and release of their health care information in violation of ME. STAT. tit. 22, §1711-C (2).

331. Plaintiff Colby, individually and on behalf of the Maine Sub-Class, seeks relief including but not limited to actual damages, injunctive relief, and/or attorneys' fees and costs under ME. STAT. tit. 22, §1711-C (13)(B).

COUNT XVI
Violation of the Maryland Consumer Protection Act, MD. CODE, COM. LAW §§13-101, *et seq*.
(On Behalf of Plaintiff Buechler and the Maryland Sub-Class)

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

333. Shields is a "person" as defined by Md. Comm. Code §13-101(h).

334. Shields' conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by MD. CODE, COM. LAW §§13-101(i) and 13-303.

335. Plaintiff Buechler and Maryland Sub-Class Members are "consumers" as defined by MD. CODE, COM. LAW §13-101(c).

336. Shields advertises, offers, or sell "consumer goods" or "consumer services" as defined by MD. CODE, COM. LAW §13-101(d).

337. Shields advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

338. The Maryland Consumer Protection Act ("MCPA") provides that a person may not engage in any unfair or deceptive trade practice in the sale of any consumer good. MD. CODE, COM. LAW §13-303. Shields participated in misleading, false, or deceptive acts that violated the MCPA.

339. Shields engaged in unfair and deceptive trade practices, in violation of MD. CODE, COM. LAW §13-301, including:

a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

b. Representing that consumer goods or services have a characteristic that they do not have;

c. Representing that consumer goods or services are of a particular standard, quality, or grade that they are not;

d. Failing to state a material fact where the failure deceives or tends to deceive;

e. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered; and

f. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

340. Shields engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services or with respect to the provision of human resources services, in violation of MD. CODE, COM. LAW §13-303, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Buechler and Maryland Sub-Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Buechler and Maryland Sub-Class Members' Private Information, including duties imposed by, inter alia, the FTCA, 15 U.S.C. §45, and the Maryland Personal Information Protection Act ("MPIPA"), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Buechler and Maryland Sub-Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Buechler and Maryland Sub-Class Members' Private Information, including duties imposed by, inter alia, the FTCA, 15 U.S.C. §45, and the MPIPA;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Buechler and Maryland Sub-Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Buechler and Maryland Sub-Class Members' Private Information, including duties imposed by, inter alia, the FTCA, 15 U.S.C. §45, and the MPIPA.

341. Shields' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Shields' data security and ability to protect the confidentiality of consumers' Private Information.

342. Had Shields disclosed that its data systems were not secure and, thus, vulnerable to attack, Plaintiff Buechler and Maryland Sub-Class Members would have been able to protect themselves against Shields' vulnerable systems (*i.e.*, by avoiding their services) and Shields would have been unable to continue in business and it would have been forced to adopt reasonable data

security measures that comply with the law and industry standards. Instead, Shields held itself out as a company that has expertise in legal compliance, and Shields was trusted with sensitive and valuable Private Information regarding thousands of consumers, including Plaintiff Buechler and the Maryland Sub-Class. Shields accepted the responsibility of being a bailee of sensitive data while keeping the inadequate state of its security controls secret from the public.

343. Shields acted intentionally, knowingly, and maliciously to violate the MCPA, and recklessly disregarded Plaintiff Buechler and Maryland Sub-Class Members' rights. Given the large number of recent high-profile data breaches, Shields knew or should have known that its security and privacy protections were inadequate.

344. As a direct and proximate result of Shields' unfair and deceptive acts and practices, Plaintiff Buechler and Maryland Sub-Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

345. Plaintiff Buechler, individually and on behalf of the Maryland Sub-Class, seeks all monetary and nonmonetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

COUNT XVII
Violation of the Maryland Personal Information Protection Act,
MD. CODE, COM. LAW §§14-3501, *et seq*.
(On behalf of Plaintiff Buechler and the Maryland Sub-Class)

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

347. Under the Maryland Personal Information Protection Act ("MPIPA"), "[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations." MD. CODE, COM. LAW §14-3503(a).

348. Shields is a business that owns or licenses "computerized data" that includes Personal Information as defined by MD. CODE, COM. LAW §§14-3501(b)(1) and (2).

349. Plaintiff Buechler and Maryland Sub-Class Members are "individuals" and "customers" as defined and covered by MD. CODE, COM. LAW §§14-3502(a) and 14-3503.

350. Plaintiff Buechler and Maryland Sub-Class Members' Personal Information includes Personal Information as covered under MD. CODE, COM. LAW § 14-3501(d).

351. Shields did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of MD. CODE, COM. LAW § 14-3503.

352. The Data Breach was a "breach of the security of a system" as defined by Md. Comm. Code §14-3504(1).

353. Under MD. CODE, COM. LAW §14-3504(b)(1), "[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach."

354. Under MD. CODE, COM. LAW §§14-3504(b)(2) and 14-3504(c)(2), "[i]f, after the investigation is concluded, the business determines that misuse of the individual's Personal Information has occurred or is reasonably likely to occur as a result of a breach of the security of a system, the business shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical after the business discovers or is notified of the breach of the security of a system."

355. Because Shields discovered a security breach, it had an obligation to disclose the breach in a timely and accurate fashion as mandated by MD. CODE, COM. LAW §§14-3504(b)(2) and 14-3504(c)(2). It did not do this, instead waiting multiple months to disclose and inform consumers of the breach.

356. By failing to disclose the breach in a timely and accurate manner, Shields violated MD. CODE, COM. LAW §§14-3504(b)(2) and 14-3504(c)(2).

357. As a direct and proximate result of Shields' violations of the MPIPA, Plaintiff Buechler and Maryland Sub-Class Members suffered damages, as described herein.

358. Pursuant to MD. CODE, COM. LAW §14-3508, Shields' violations of MD. CODE, COM. LAW §§14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the MCPA, MD. CODE, COM. LAW §§13-101, *et seq*. and subject to the enforcement and penalty provisions contained within the MCPA.

359. Plaintiff Buechler, individually and on behalf of the Maryland Sub-Class, seeks relief under MD. CODE, COM. LAW §13-408, including actual damages and attorney's fees.

COUNT XVIII
Violation of the Maryland Social Security Number Privacy Act,
MD. CODE, COM. LAW §§4-3401, *et seq*.
(On Behalf of Plaintiff Buechler and the Maryland Sub-Class)

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

361. Shields is a "person" as covered by MD. CODE, COM. LAW §14-3402.

362. Plaintiff Buechler and Maryland Sub-Class Members are "individual[s]" covered by MD. CODE, COM. LAW §14-3402.

363. MD. CODE, COM. LAW §14-3402 prohibits a person from requiring an individual to transmit his/her Social Security number over the Internet unless the connection is secure or the individual's Social Security number is encrypted, and from initiating the transmission of an individual's Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted.

364. As described above, Shields transmitted Plaintiff Buechler and Maryland Sub-Class Members' Social Security numbers over the Internet on unsecure connections and/or without encrypting the Social Security Numbers in violation of MD. CODE, COM. LAW §14-3402.

365. As a direct and proximate result of Shields' violations of Md. Comm. Code §14-3402, Plaintiff Buechler and Maryland Sub-Class Members suffered damages described above.

366. Plaintiff Buechler, individually and on behalf of the Maryland Sub-Class, seeks relief under MD. CODE, COM. LAW §14-3402, including actual damages and attorneys' fees.

COUNT XIX
Violation of the New Hampshire Consumer Protection Act,
N.H. REV. STAT. §§358-A, *et seq*.
(On Behalf of Plaintiff Tapper and the New Hampshire Sub-Class)

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

368. Shields is considered a "person" under the New Hampshire Consumer Protection Act ("NHCPA"). N.H. REV. STAT. §358-A:1(I).

369. The NHCPA prohibits a person or entity from using "any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce within this state." N.H. REV. STAT. §358-A:2.

370. The New Hampshire statutory scheme provides a non-exhaustive list of acts that constitute violations of the statute, which includes but is not limited to the following:

a. "Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that such person does not have." N.H. REV. STAT. §358-A:2(V).

b. "Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another." N.H. REV. STAT. §358-A:2(VII).

c. "Advertising goods or services with intent not to sell them as advertised." N.H. REV. STAT. §358A:2(IX).

371. The New Hampshire Supreme Court has held that conduct that is not specifically delineated within the statutory scheme is analyzed under the "rascality test." *Axenics, Inc. v. Turner Constr. Co.*, 62 A.3d 754, 768-69 (N.H. 2013).

372. Defendant engaged in the conduct alleged in this complaint through transactions in and involving trade and commerce within the State of New Hampshire. N.H. REV. STAT. §358-A:2.

373. While involved in trade or commerce, Defendant violated the NHCPA by engaging in unfair, deceptive, and unconscionable business practices including, among other things, by:

a. Failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect the Private Information of Defendant's patients from unauthorized access and disclosure;

b. Failing to disclose the material fact that its computer systems and data security practices were inadequate to safeguard and protect the Private Information of Plaintiff Tapper and New Hampshire Sub-Class from being compromised, stolen, lost, or misused; and

c. Failing to disclose the Data Breach to Plaintiff Tapper and New Hampshire Sub-Class Members "as soon as possible" in violation of N.H. REV. STAT. §359-C:20(I)(a).

374. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff Tapper and New Hampshire Sub-Class Members' Private Information entrusted to it, and that risk of a data breach or theft was highly likely.

375. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

376. Defendant's failures constitute an unfair practice and false, deceptive, and misleading representations regarding the security of Defendant's network and aggregation of Private Information.

377. These unfair practices and misleading representations upon which impacted individuals (including Plaintiff Tapper and New Hampshire Sub-Class Members) relied were material facts (*e.g.*, as to Defendant's adequate protection of Private Information), and consumers (including Plaintiff Tapper and New Hampshire Sub-Class Members) relied on those representations to their detriment.

378. In committing the acts alleged herein, Defendant engaged in fraudulent, deceptive, and unfair practices by omitting, failing to disclose, or inadequately disclosing to Plaintiff Tapper

and New Hampshire Sub-Class Members that Shields did not follow industry best practices for the collection, use, and storage of Private Information.

379. Defendant's conduct, as described herein, constitutes willful and/or knowing violations of the NHCPA.

380. As a direct and proximate result of Defendant's conduct, Plaintiff Tapper and New Hampshire Sub-Class Members have been harmed and have suffered damages including, but not limited to: damages arising from attempted identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

381. As a direct and proximate result of Defendant's fraudulent, deceptive, and unfair practices and omissions, Plaintiff Tapper and New Hampshire Sub-Class Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff Tapper and New Hampshire Sub-Class Members damages. Accordingly, Plaintiff Tapper and New Hampshire Sub-Class Members are entitled to recover damages in accordance with the NHCPA, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs.

COUNT XX
Violation of the New Hampshire Notice of Security Breach statute, N.H. REV. STAT.§§359-C:20, *et seq*.
(On Behalf of Plaintiff Tapper and the New Hampshire Sub-Class)

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

383. The New Hampshire Notice of Security Breach statute states that:

> Any person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required . . . .

N.H. REV. STAT. §359-C:20(I)(a).

384. Shields is a business that own or license computerized data that includes Personal Information, of Plaintiff Tapper and New Hampshire Sub-Class Members, as defined by N.H. REV. STAT. §359-C:20(I)(a).

385. Plaintiff Tapper and New Hampshire Sub-Class Members' Private Information (*e.g.*, a person's first and last name, and their Social Security number) includes Personal Information as covered under N.H. REV. STAT. §359-C:19(IV)(a).

386. Defendant acted as a licensee of the sensitive Private Information in using it in the regular course of business and by storing this valuable and highly sensitive information on its computer systems and network.

387. Per N.H. REV. STAT. §359-C:20(I)(a), Defendant was required to "notify the affected individuals as soon as possible" of the Data Breach. Although Plaintiff Tapper and New Hampshire Sub-Class Members' Private Information was included in the Data Breach and compromised, Defendant failed to send the requisite notice under New Hampshire law as soon as possible.

388. In failing to timely disclose the Data Breach, Defendant harmed Plaintiff Tapper and New Hampshire Sub-Class Members because Plaintiff Tapper and New Hampshire Sub-Class Members were not able to immediately take precautionary action to prevent and mitigate the effects of identity theft and financial fraud.

389. By failing to disclose the Data Breach in a timely and reasonable manner, Defendant violated N.H. REV. STAT. §359-C:20(I)(a).

390. As a direct and proximate result of Defendants' violation of the notice requirement under N.H. REV. STAT. §359-C:20(I)(a), Plaintiff Tapper and New Hampshire Sub-Class Members suffered the above-mentioned damages. Accordingly, Plaintiff Tapper and New Hampshire Sub-Class Members are entitled to recover actual damages, injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

COUNT XXII

Violation of the Massachusetts Consumer Protection Act, MASS. GEN. LAWS ch. 93A, §§1, *et seq*.
(On Behalf of Plaintiffs and the Class)

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

392. Defendant is a "person" as defined by the Massachusetts Consumer Protection Act, MASS. GEN. LAWS ch. 93A, §1.

393. Defendant is engaged in "trade" or "commerce" defined as 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.

394. Defendant is engaged in trade or commerce that directly or indirectly affects the people of the Commonwealth of Massachusetts.

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

396. Defendant misrepresented that it would keep the Private Information of Plaintiffs and the Class Members secure, private, and confidential.

397. Defendant had a duty to keep the Private Information safe and secure under HIPAA and regulations promulgated thereunder, the FTCA and regulations promulgated thereunder, and MASS. GEN. LAWS ch. 93H, §2 and regulations promulgated thereunder.

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

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

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

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

402. Criminals were able to access Private Information through the Data Breach.

403. 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, the Massachusetts Security Breach statute.

404. Although it was aware of the Data Breach, Defendant failed to timely notify its patients of the breach, including Plaintiffs and members of the Class.

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

406. As a result of the aforementioned actions and omissions, Plaintiffs and members of 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.

407. 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.

408. A demand 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.

PRAYER FOR RELIEF

A. That the Court certify this action as a class action and certify the Class and sub-classes, as proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are a proper class and sub-class representatives; and appoint Plaintiffs' Counsel as Class and Sub-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 Plaintiffs and members of the Classes and Sub-classes 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. (*admitted pro hac vice*)
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

David J. George
GEORGE GESTEN MCDONALD, PLLC
9897 Lake Worth Road, Suite 302
Lake Worth, FL 33467
Telephone: (561) 232-6002
dgeorge@4-justice.com

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

Elizabeth Pollock-Avery (*admitted pro hac vice*)
Gary F. Lynch (*admitted pro hac vice*)
Hannah N. Barnett (*admitted pro hac vice*)
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 (*admitted pro hac vice*)
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 (admitted pro hac vice)
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
|One North Broadway, Suite 900
White Plains, New York 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 (*admitted pro hac vice*)
Erin Green Comite (*admitted pro hac vice*)
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, Illinois 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