UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

DEBRA MONETTE, on Behalf of Herself and All Others Similarly Situated, Plaintiff, v. SHIELDS HEALTH CARE GROUP, INC., Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Debra Monette ("Plaintiff") brings this Class Action Complaint on behalf of herself and all others similarly situated, against Defendant Shields Health Care Group, Inc. ("Shields" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to her, which are based on her personal knowledge:

NATURE OF THE CASE

1. Plaintiff brings this class action on behalf of herself and a class of individuals who used Shields's services whose personally identifying information ("PII") and/or protected health information ("PHI") were accessed and exposed to unauthorized third parties during a data breach of Shields's system, which Shields states occurred between March 7, 2022 and March 28, 2022 (the "Data Breach") and involved the "management and imaging services" Shields provides for approximately 56 distinct "Facility Partners."

2. On March 28, 2022, Shields was alerted to suspicious activity that may have involved a breach of its systems. Shields admitted that an unknown actor gained access to certain Shields systems from March 7, 2022 to March 21, 2022, and that certain data was exfiltered by the

unknown actor. The data breach impacted two million people and more than 50 of Shields's health care facilities.

3. Healthcare providers that handle sensitive PII or PHI owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII or PHI to unauthorized persons – and especially hackers with nefarious intentions – will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

4. The harm resulting from a data breach manifests in a number of ways, including identity theft and financial fraud. The exposure of a person's PII or PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk – to the extent it is even possible to do so – requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take a number of additional prophylactic measures.

5. As a healthcare provider, Shields knowingly obtains patient PII and PHI and has a resulting duty to securely maintain such information in confidence.

6. Shields's Privacy Practice informs patients "how medical information about [patients] may be used and disclosed how and [they] can get access to [that] information."[1] The Privacy Practice acknowledges Shields's duty to maintain the privacy of patients' health information.

[1] *Privacy*, SHIELDS HEALTH CARE GROUP, https://shields.com/privacy/ (last visited July 12, 2022).

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

8. Plaintiff, on behalf of herself and the Class as defined herein, brings claims for negligence, negligence *per se*, breach of fiduciary duty, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

9. Based on the public statements of Shields to date, a wide variety of PII and PHI were implicated in the breach, including full name, Social Security number, date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient identification ("ID"), and other medial or treatment information.[3]

10. As a direct and proximate result of Shields's inadequate data security, and its breach of its duty to handle PII and PHI with reasonable care, Plaintiff and Class members' PII and PHI have been stolen by hackers and exposed to an untold number of unauthorized individuals.

11. Plaintiff and Class members now face an imminent significantly increased risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief. These risks may last for the rest of their lives. Consequently, Plaintiff and Class members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

---

[2] *Notice of Data Security Incident*, SHIELDS HEALTH CARE GROUP, https://shields.com/notice-of-data-security-incident/ (last visited July 12, 2022).

[3] *Id.*

12. To recover from Shields for these harms, Plaintiff and the Class seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Shields to: (1) disclose, expeditiously, the full nature of the Data Breach and the types of PII and PHI accessed, obtained, or exposed by the hackers; (2) implement improved data security practices to reasonably guard against future breaches of PII and PHI possessed by Shields; and (3) provide, at its own expense, all impacted victims with identity theft protection services.

PARTIES

Plaintiff

13. Plaintiff Debra Monette is an adult individual who at all relevant times has been a citizen and resident of the Commonwealth of Massachusetts and was a patient of Defendant's, receiving services at the following facilities:

a. Memorial Marlborough Hospital, located at 157 Union Street, Marlborough, Massachusetts 01752; and

b. Shields MRI Framingham, located at 14 Cochituate Road, Framingham, Massachusetts 01701.

14. As a result of the Data Breach, Plaintiff has had her PII and PHI stolen by hackers and exposed to an untold number of unauthorized individuals.

Defendant

15. Defendant Shields Health Care Group, Inc. is a Massachusetts corporation with its principal place of business located at 700 Congress Street, #204, Quincy, Massachusetts 02169 in this District.

JURISDICTION AND VENUE

16. This Court has jurisdiction over this action pursuant to 28 U.S.C. §1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

17. This Court has personal jurisdiction over Defendant because Defendant has its principal place of business in Massachusetts and a substantial part of the events arising out of the claims alleged herein occurred within the District.

18. Venue is proper in this District, pursuant to 28 U.S.C. §1391(b)(1), because a substantial part of the acts, omissions, and events giving rise to Plaintiff's claims occurred in this District. Further, Defendant has its principal place of business in this District.

FACTUAL BACKGROUND

A. Shields Health Care Group and the Services Provided

19. Shields is a for-profit company that provides management and imaging services on behalf of several dozen partner facilities in the New England region, including Massachusetts, Maine, and New Hampshire.[4]

20. Shields provides services such as MRI, PET/CT, ASC, Radiation Oncology, and Ambulatory Surgical Centers.[5]

21. The company provides services to many thousands of patients a year.

---

[4] *Find a Location*, SHIELDS HEALTH CARE GROUP, https://shields.com/find-location/ (last visited July 12, 2022).

[5] *Our Services*, SHIELDS HEALTH CARE GROUP, https://shields.com/our-services/overview/ (last visited July 12, 2022).

22. While administering these services and treatment, Defendant on a daily basis receives, creates, and handles PII and PHI, which includes, *inter alia*, patients' full name, address, date of birth, Social Security number, other contact information, diagnosis, billing information, insurance information, medical records, patient ID, and other necessary information for treatment at the facilities.

23. Patients must entrust their PII and PHI to Defendant to receive care, and in return, they reasonably expect that Defendant will safeguard their highly sensitive information and keep their PHI confidential.

24. Defendant refers to patients' information as "protected health information" and promises disclosure of highly sensitive personal information will only occur for the "purpose[] of treatment, payment or health care operations."[6]

B. Shields Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims

25. At all relevant times, Shields knew it was storing sensitive PII and PHI and that, as a result Shields's systems would be attractive for cybercriminals.

26. Shields also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

27. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

---

6 *See supra*, n.1.

28. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as well as the "proliferation of open and anonymous cybercrime forums on the Dark Web that server as a bustling marketplace for such commerce."[7] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

29. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the United States. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[8]

30. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[9]

31. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[10]

---

[7] Brian Krebs, *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[8] *Data Breach Report: 2021 Year End*, RISK BASED SECURITY (February 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/.

[9] *Facts + Statistics: Identity theft and cybercrime*, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited July 12, 2022).

[10] *9 reasons why healthcare is the biggest target for cyberattacks*, SWIVEL SECURE, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited July 12, 2022).

32. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it quickly – making the industry a growing target."[11]

33. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Shields's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

34. As indicated by Jim Trainor, former second in command at the Federal Bureau of Investigation's cyber security division:

> Medical records are a gold mine for criminals – they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. "Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to – we've even seen $60 or $70."[12]

A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[13]

35. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.

---

11 *Id.*

12 *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDEXPERTS (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

13 PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*: *Key findings from The Global State of Information Security® Survey 2015*, PRICEWATERHOUSECOOPERS (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[14]

36. 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 [Dark] 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.[15]

37. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

38. Shields certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

---

[14] Brian O'Connor, *Healthcare Data Breach: What to Know About Them and What to Do After One*, EXPERIAN (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

[15] U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However the Full Extent Is Unknown* (June 2007).

C. Shields Breached Its Duty to Protect Its Patients' PII and PHI

39. On or around June 7, 2022, Defendant released a "Notice of Data Security Incident" that announced that on or around March 28, 2022, Defendant was alerted to suspicious activity and that an unknown actor gained access to Shields's system from approximately March 7, 2022 to March 21, 2022.[16]

40. According to Shields, it is reviewing the extent of the breach and alleges there is no evidence to indicate that the PII or PHI exfiltered during the breach was used to commit fraud,[17] but based on the amount of sensitive information Shields possesses, it would be naïve to believe the cybercriminals did not purposefully steal sensitive PII and PHI with a specific intent to use it or sell it to others who will.

41. Defendant determined that the information that was impacted included full name, Social Security number, date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient ID, and other medial or treatment information.[18]

42. The unauthorized persons gained access to the PII and PHI of approximately two million patients.[19]

43. While the Data Breach occurred in March, Defendant alerted the public and its patients in the beginning of June, two full months after the Breach. In those months, Shields left the public in the dark; it failed to inform patients the danger posed by the ongoing breach. Even

---

16 *See supra*, n.2.

17 *Id.*

18 *Id.*

19 Marc Fortier, *2 million Impacted by Data Breach at Massachusetts Health Care Organization*, 10 NBC BOSTON (June 8, 2022), https://www.nbcboston.com/news/local/massachusetts-health-care-group-investigating-data-security-breach/2741994/.

now, Shields's disclosures have been vague and evasive, leaving Plaintiff and Class members with incomplete information regarding the true nature and extent of the data breach.

44. The Data Breach occurred as a direct result of Shields's failure to implement and follow basic security procedures in order to protect its patients' PII and PHI.

45. Shields says it "takes the confidentiality, privacy, and security information in [their] care seriously" yet alerts its patients of the Data Breach while it is too late for patients to safeguard their information and provides no assistance to its patients in the event of their identity being stolen.[20]

46. Plaintiff did not receive a personal notice of the Data Breach, but instead learned of the Breach through the internet.

D. Plaintiff and Class Members Suffered Damages

47. For the reasons mentioned above, Shields's conduct, which allowed the Data Breach to occur, caused the Plaintiff and members of the Class significant injuries and harm in several ways. Plaintiff and members of the Class must immediately devote time, energy, and money to: (1) closely monitor their medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

[20] *See supra*, n.2.

48. Shortly after the Breach, Plaintiff received notification from her bank of attempted fraudulent activity on her bank account. As a result, Plaintiff devoted time and energy to change her bank account numbers and ensure that her account was secure.

49. Once PII and PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Shields's conduct. Further, the value of Plaintiff and Class members' PII and PHI has been diminished by its exposure in the Data Breach.

50. As a result of Shields's failures, Plaintiff and Class members are subject to an imminent substantial increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

51. Plaintiff and Class members are also at a continued risk because their information remains in Shields's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Shields fails to undertake the necessary and appropriate security and training measures to protect its patients' PII and PHI.

52. Plaintiff and Class members have been injured and have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their PII and PHI to hackers and other unauthorized parties.

CLASS ALLEGATIONS

53. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following class:

> All individuals in the United States and its territories whose PII and/or PHI was compromised in the Shields Health Care Group data breach which occurred on or about March 7, 2022 until on or about March 21, 2022 (the "Class").

54. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

55. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

56. The requirements of Rule 23(a)(1) are satisfied. The Class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class members through this class action will benefit both the parties and this Court. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach, but based on public information, the Class includes approximately two million individuals.

57. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest, and there are common questions of fact and law affecting members of the Class. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether Defendant had a duty to protect the PII and PHI of Plaintiff and Class members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class members' PII and PHI, and breached its duties thereby;

c. Whether Defendant breached its fiduciary duty to Plaintiff and the Class;

d. Whether Plaintiff and Class members are entitled to damages as a result of Defendant's wrongful conduct; and

e. Whether Plaintiff and Class members are entitled to restitution as a result of Defendant's wrongful conduct.

58. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the members of the Class. The claims of Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard PII and PHI.

59. Plaintiff and members of the Class were all patients of Shields, each having their PII and PHI obtained by an unauthorized third party.

60. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class members are substantially identical as explained above.

61. The requirements of Rule 23(b)(3) are satisfied here because a class action is the superior method of litigation for these issues, and common issues will predominate. While the aggregate damages that may be awarded to the members of the Class are likely to be substantial, the damages suffered by the individual members of the Class are relatively small. As a result, the

expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a Class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff and the Class, and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class member.

FIRST CAUSE OF ACTION

NEGLIGENCE
(On Behalf of Plaintiff and the Class)

62. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

63. Shields owed a duty under common law to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

64. Shields's duty to use reasonable care arose from several sources, including but not limited to those described below.

65. Shields had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable PII and PHI that is routinely targeted by criminals for unauthorized access, Shields was obligated to act with reasonable care to protect against these foreseeable threats.

66. Shields's duty also arose from Shields's position as a healthcare provider. Shields holds itself out as a trusted provider of healthcare, and thereby assumes a duty to reasonably protect its patients' information. Indeed, Shields, which directly manages imaging and management services, was in a unique and superior position to protect against the harm suffered by Plaintiff and Class members as a result of the Data Breach.

67. Shields breached the duties owed to Plaintiff and Class members and thus was negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, Shields breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

68. But for Shields's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their PII and PHI would not have been compromised.

69. As a direct and proximate result of Shields's negligence, Plaintiff and Class members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Shields with the mutual understanding that Shields would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; and

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Shields's possession and is subject to further breaches so long as Shields fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data.

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

70. As a direct and proximate result of Shields's negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION

NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

71. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

72. Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act") prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by entities such as Shields for failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Shields's duty.

73. Shields violated §5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Shields's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of a data breach involving PII and PHI of its patients.

74. Shields's violation of §5 of the FTC Act constitutes negligence *per se*.

75. Plaintiff and members of the Class are consumers within the class of persons §5 of the FTC Act was intended to protect.

76. Shields is an entity covered under the Health Insurance Portability and Accountability Act ("HIPAA"), which sets minimum federal standards for privacy and security of PHI.

77. Pursuant to HIPAA, 42 U.S.C. §§1302d, *et seq.*, and its implementing regulations, Shields had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class members' electronic PHI.

78. Specifically, HIPAA required Shields to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 C.F.R. §§164.102, *et seq*.

79. HIPAA also requires Shields to provide Plaintiff and the Class members with notice of any breach of their individually identifiable PHI "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach." 45 C.F.R. §§164.400-414.

80. Shields violated HIPAA by actively disclosing Plaintiff's and the Class members' electronic PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PHI; and by failing to provide Plaintiff and Class members with notification of the Data Breach within 60 days after its discovery.

81. Plaintiff and the Class members are patients within the class of persons HIPAA was intended to protect.

82. Shields's violation of HIPAA constitutes negligence *per se*.

83. The harm that has occurred as a result of Shields's conduct is the type of harm that the FTC Act and HIPAA was intended to guard against.

84. As a direct and proximate result of Shields's negligence, Plaintiff's and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION

BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

85. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

86. Plaintiff and Class members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by Shields, and that was ultimately accessed or compromised in the Data Breach.

87. As a healthcare provider, Shields has a fiduciary relationship to its patients, like Plaintiff and the Class members.

88. Because of that fiduciary and special relationship, Shields was provided with and stored private and valuable PHI related to Plaintiff and the Class.

89. Shields owed a fiduciary duty under common law to Plaintiff and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

90. Shields breached the duties owed to Plaintiff and Class members and thus was negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, Shields breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

91. But for Shields's wrongful breach of its duties owed to Plaintiff and Class members, their PII and PHI would not have been compromised.

92. As a direct and proximate result of Shields's negligence, Plaintiff and Class members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Shields with the mutual understanding that Shields would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; and

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Shields's possession and is subject to further breaches so long as Shields fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data.

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

93. As a direct and proximate result of Shields's breach of its fiduciary duty, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION

DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

94. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

95. 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.

96. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class members' PII and PHI and whether Shields is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Shields's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and PHI and remains at imminent risk that further compromises of her PII and/or PHI will occur in the future.

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

a. Shields owes a legal duty to secure patients' PII and PHI and to timely notify patients of a data breach under the common law, §5 of the FTC Act and HIPAA.

b. Shields breached and continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

98. 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' PII and PHI.

99. If an injunction is not issued, Plaintiff 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, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and she and the Class members will be forced to bring multiple lawsuits to rectify the same conduct.

100. The hardship to Plaintiff and the Class members if an injunction does not issue exceeds the hardship to Shields if an injunction is issued. Plaintiff 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.

101. 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 Plaintiff, Class members, and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all other similarly situated, prays for relief as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. For damages in an amount to be determined by the trier of fact;

D. For an order of restitution and all other forms of equitable monetary relief;

E. Declaratory and injunctive relief as described herein;

F. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

G. Awarding pre- and post-judgment interest on any amounts awarded; and

H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Respectfully Submitted,

Dated: July 13, 2022

s/ *Joseph P. Guglielmo*
Joseph P. Guglielmo BBO #671410
Carey Alexander (*pro hac vice* forthcoming)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: 212-223-6444
Facsimile: 212-233-6334
jguglielmo@scott-scott.com
calexander@scott-scott.com

Erin Green Comite (*pro hac vice* forthcoming)
SCOTT+SCOTT ATTORNEYS AT LAW LLP
156 S. Main Street
P.O. Box 192
Colchester, CT 06415
Telephone: 860-531-2632
Facsimile: 860-537-4432
ecomite@scott-scott.com

Counsel for Plaintiff