UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

WILLIAM BISCAN, individually and on behalf of all others similarly situated, Plaintiff, v. SHIELDS HEALTH CARE GROUP INC., Defendant.	**CIVIL ACTION NO.: _____** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff William Biscan, ("Plaintiff") individually and on behalf of all others similarly situated, bring this action against Defendant Shields Health Care Group Inc. ("Shields" or "Defendant"), a Massachusetts corporation, to obtain damages, restitution, and injunctive relief for himself and for the Class, as defined below, from Defendant.

Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This class action arises out of a targeted cyber-attack at Defendant's medical facilities that allowed a third party to access Defendant's computer systems and data from approximately March 7, 2022 to March 21, 2022, exposing highly sensitive personal information and medical records of approximately two million patients from Defendant's computer network (the "Data Breach").

2. As a result of the Data Breach, Plaintiff 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.

3. Plaintiff's and Class Members' sensitive and private personal information—which was entrusted to Defendant, its officials, and agents—was compromised, unlawfully accessed, and stolen as a result of 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, and other protected health information as defined by the HIPAA, and other personally identifiable information ("PII") and protected health information ("PHI") that Defendant collected and maintained (collectively, "Private Information").

4. Plaintiff brings this class action lawsuit on behalf of all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that Defendant collected and maintained, for failing to provide timely and adequate notice to Plaintiff 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.

5. Defendant owed a duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their Private Information against unauthorized access and disclosure.

6. Defendant breached its duty to Plaintiff and Class Members by maintaining Plaintiff's and the Class Members' Private Information in a negligent and/or reckless manner.

7. Upon information and belief, the means of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information were known and foreseeable risks to Defendant, and 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.

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

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

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

11. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including 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 on 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.

12. As a direct result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiff and Class Members 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.

14. As a direct and proximate result of the Data Breach and subsequent exposure of

their Private Information, Plaintiff 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 e-mails received as a result of the Data Breach. Plaintiff and Class Members have suffered and will continue to suffer an invasion of their property interest in their own PII and PHI such that they are entitled to damages from Defendant for unauthorized access to, theft of, and misuse of their PII and PHI. These harms are ongoing, and Plaintiff and Class Members will suffer from future damages associated with the unauthorized use and misuse of their PII and PHI as thieves will continue to use the information to obtain money and credit in their names for several years.

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

16. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring/identity protection services funded by Defendant.

17. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct asserting claims for negligence, breach of contract, breach of implied contract, invasion of privacy, breach of fiduciary duty, breach of confidence, violation of the Massachusetts Regulation of Business Practices for Consumers' Protection Act, Mass. Gen. Laws Ann. ch. 93A, § 1 *et seq*., and unjust enrichment.

PARTIES

18. Plaintiff Biscan is, and at all times mentioned herein was, an individual citizen of

Haverhill, Massachusetts. Plaintiff Biscan was a patient of Shields through its services at Winchester Hospital / Shields MRI, LLC.

19. Defendant Shields Health Care Group Inc. is a domestic corporation organized and existing under the laws of the Commonwealth of Massachusetts with its headquarters in Quincy, Massachusetts.

JURISDICTION AND VENUE

20. This Court has personal jurisdiction over Defendant because Defendant is a resident of the Commonwealth of Massachusetts and because Defendant conducts business transactions in Massachusetts, has committed tortious acts in Massachusetts, and sells its products and services in Massachusetts. The Court has personal jurisdiction over Plaintiff because he resides in the Commonwealth of Massachusetts.

21. Jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d), as minimal diversity exists, there are more than 100 class members, and the amount in controversy is in excess of $5 million.

FACTUAL ALLEGATIONS

Defendant's Business

22. Defendant is "the largest network of MRI centers in New England,"[1] with "more than 40 healthcare facilities throughout New England" including locations in Massachusetts, Maine, and New Hampshire.[2]

23. Defendant's business includes providing MRI, PET/CT, Radiation Oncology, and

[1] Shields Health Care Group, *Our Services*, available at https://shields.com/our-services/overview/ (last accessed June 9, 2022).
[2] Shields Health Care Group, *Find a Location*, available at https://shields.com/find-location/ (last accessed June 9, 2022)

Ambulatory Surgical Center services.[3]

24. In the ordinary course of receiving medical services and treatment from Defendant, patients are required to provide (and Plaintiff did in fact provide) Defendant with sensitive, personal, and private information such as:

- Name and address;
- Date of birth;
- Demographic information;
- Social Security number;
- Information relating to individual medical history;
- Insurance information and coverage;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Photo identification;
- Other information that may be deemed necessary to provide care.

25. Defendant also gathers certain medical information about patients and creates records of the care it provides them.

26. Additionally, Defendant may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patients' health plan(s), close friends, and/or family members.

Defendant Represented to Plaintiff and Class Members That It Would Adequately Protect Their Private Information

27. Defendant boasts that "Shields takes the confidentiality, privacy, and security of

[3] Shields Health Care Group, *Our Services*, available at https://shields.com/our-services/overview/ (last accessed June 9, 2022).

information in our care seriously."[4]

28. Defendant has promulgated and adopted a privacy practice that it represents to patients it follows with respect to their Private Information (the "Privacy Practice"). The Privacy Practice is posted on Defendant's website, and is provided to each patient prior to treatment.[5]

29. In the Privacy Practice, Defendant states that Defendant "will generally only disclose health information about [patients] for the purposes of treatment, payment or health care operations" and specifically lists examples of how Defendant will use this information.[6] The uses described in the Privacy Practice do not include exposure to cybercriminals.

30. Defendant also represents to patients in its Privacy Practice that it will "[m]aintain the privacy of your health information as required by law."[7]

31. Defendant expressly represents to patients that Defendant is required to "abide by the terms of this [Privacy Practice]."[8]

32. Plaintiff and Class Members are, or were, patients of Defendant or received health-related services from Defendant, and entrusted Defendant with their Private Information.

The Data Breach

33. From approximately March 7, 2022 to March 21, 2022, Defendant experienced a targeted cybersecurity incident where cyberthieves had unauthorized access to the Defendant network for approximately two weeks.[9] Defendant investigated a data security alert at least as early

[4] Shields Health Care Group, *Notice of Data Security Incident*, available at https://shields.com/notice-of-data-security-incident/ (last accessed June 9, 2022).
[5] *See* Shields Health Care Group, *Privacy*, available at https://shields.com/privacy/ (last accessed June 9, 2022).
[6] *Id*.
[7] *Id*.
[8] *Id*.
[9] Shields Health Care Group, *Notice of Data Security Incident*, available at https://shields.com/notice-of-data-security-incident/ (last accessed June 9, 2022).

as March 18, 2022.[10]

34. Upon information and belief, the cyber-attack was "soft targeted" at Defendant, due to Defendant's status as a healthcare entity that collects, creates, and maintains both PII and PHI. The "soft targeted" cyber-attack was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of patients like Plaintiff and Class Members.

35. Defendant's investigation into the Data Breach found that cybercriminals had been able to access patient files that that included names, addresses, dates of birth, Social Security numbers, patient ID numbers, insurance information, and/or medical information related to care received.[11]

36. At minimum, due to inadequate security precautions, between the date range March 7, 2022 and March 21, 2022, the PII and PHI of approximately two million patients was exposed.[12]

37. Despite investigating the Data Breach on or about March 18, 2022, Defendant did not publish a press release regarding the Data Breach until approximately June 7, 2022, stating the information that was accessed 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 medical or treatment information."[13]

38. This was the first notice of the Data Breach that Shields provided to its patients.

39. Based on Defendant's disclosures, Plaintiff believes his Private Information was

---

[10] *Id*.
[11] *Id*.
[12] Associated Press, *Data breach at health care organization may affect 2 million*, available at https://apnews.com/article/technology-health-us-department-of-and-human-services-boston-massachusetts-4aed357bc7f3fd0a8a88f40d13985fdf (last accessed June 9, 2022).
[13] Shields Health Care Group, *Notice of Data Security Incident*, available at https://shields.com/notice-of-data-security-incident/ (last accessed June 9, 2022).

stolen from Defendant's network (and subsequently sold) in the Data Breach. Ever since the Data Breach, Plaintiff Turpin has been victim of increased spam calls and phishing attempts.

40. Further, the removal of the Private Information from Defendant's system—names, addresses, dates of birth, Social Security numbers (which are the keys to identity theft and fraud), insurance information, medical record numbers, and information regarding patient care—demonstrates that this cyber-attack was targeted.

41. Cyber-attacks against healthcare organizations such as Defendant are targeted and frequent. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations. Significant security incidents are a near-universal experience in U.S. healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets."[14] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From Social Security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[15]

42. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and the Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

43. Plaintiff and the Class Members provided their Private Information to Defendant

---

14 https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last accessed June 7, 2022)

15 https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed June 7, 2022)

with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

44. By failing to protect their PII and PHI from cybercriminals, Defendant put all Class Members at risk of identity theft, financial fraud, and other serious harms.

45. Defendant negligently failed to take the necessary precautions required to safeguard and protect the PII and PHI of Plaintiff and the other Class Members from unauthorized disclosure. Defendant's actions represent a flagrant disregard of Plaintiff's and the other Class Members' rights.

This Data Breach was Foreseeable

46. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the healthcare industry preceding the date of the breach.

47. Data breaches, including those perpetrated against the healthcare sector of the economy, have become widespread.

48. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[16]

49. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[17]

50. PII and PHI are of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes.

51. PII and PHI can be used to distinguish, identify, or trace an individual's identity,

[16] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed June 7, 2022)
[17] *Id.*

such as their name, Social Security number, and medical records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.

52. Given the nature of the Data Breach, it was foreseeable that the compromised PII and PHI could be used by hackers and cybercriminals in a variety of different ways.

53. Indeed, the cybercriminals who possess the Class Members' PII and PHI can easily obtain Class Members' tax returns or open fraudulent credit card accounts in the Class Members' names.

54. Defendant was aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

55. For instance, the 525 reported medical or healthcare data breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[18]

56. Data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[19]

57. The increase in such attacks, and attendant risk of future attacks, was widely known

[18] *Id.* at p15.
[19] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed June 7, 2022).

to the public and to anyone in Defendant's industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

58. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which 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.

59. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose 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. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

60. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive 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.

61. 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. The orders resulting from these actions have further clarified the measures businesses must take to meet their data security obligations.

62. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

63. Defendant failed to properly implement basic data security practices widely known throughout the industry. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

64. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

65. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyber-attacks because of the value of the PII and PHI they collect and maintain.

66. Healthcare industry experts assert that "data breaches cost the healthcare industry approximately $5.6 billion every year[.]"

67. According to the University of Illinois Chicago (UIC), "[t]o improve cybersecurity in healthcare, organizations need to hire informatics professionals who can not only collect,

manage and leverage data, but protect it as well."[20]

68. UIC has identified several strategies and best practices that, at a minimum, should be implemented by healthcare providers like Defendant, including but not limited to: establishing a security culture; protecting mobile devices; thoroughly educating all employees; strong passwords that need to be changed regularly; multi-layer security, including firewalls, anti-virus, and anti-malware software; limiting network access; controlling physical access to devices; encryption; making data unreadable without a password or key; multi-factor authentication; backup data; and limiting employees access to sensitive and protected data.[21]

69. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security (CIS) released its Critical Security Controls, and all healthcare institutions are strongly advised to follow these guidelines.[22]

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

71. Upon information and belief, Defendant failed to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1,

[20] *See Cybersecurity: How Can It Be Improved in Health Care?*, Health Informatics-University of Illinois Chicago (last viewed: June 7, 2022), https://healthinformatics.uic.edu/blog/cybersecurity-how-can-it-be-improved-in-health-care/.
[21] *Id*.
[22] https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last accessed June 7, 2022)

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

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

72. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

73. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of sensitive patient health information. Safeguards must include physical, technical, and administrative components.

74. 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 subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

75. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

Defendant's Breach

76. Defendant breached its obligations to Plaintiff and the Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard the Defendant computer systems, network, and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords;

i. Failing to properly train and supervise employees in the proper handling of inbound emails;

j. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

l. 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)(i);

m. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

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

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

p. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

q. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

r. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had

> not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key," 45 CFR § 164.304 (definition of encryption).

77. As the result of allowing its computer systems to fall into dire need of security upgrading and its inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiff's and the Class Members' Private Information.

Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

78. Cyber-attacks at medical facilities such as Defendant's are especially problematic because of the disruption they cause to the health treatment and overall daily lives of patients affected by the attack.

79. For instance, loss of access to patient histories, charts, images, and other information forces providers to limit or cancel patient treatment due to a disruption of service.

80. This leads to a deterioration in the quality of overall care patients receive at facilities affected by cyber-attacks and related data breaches.

81. Researchers have found medical facilities that experience a data security incident incur an increase in the death rate among patients months and years after the attack.[23]

82. Researchers have further found that at medical facilities that experience a data

[23] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019) https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last accessed June 7, 2022).

security incident, the incident leads to a deterioration in patient outcomes, generally.[24]

83. Similarly, cyber-attacks and related data security incidents inconvenience patients; these inconveniences include, but are not limited, to the following:

a. rescheduling of medical treatment;

b. being forced to find alternative medical care and treatment;

c. delays or outright cancellation of medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. the indefinite loss of personal medical history.[25]

84. Cyber-attacks that result in the removal of protected data are also considered a breach under HIPAA because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. § 164.40

85. Data breaches represent a significant problem for patients who have already experienced the inconvenience and disruption associated with a cyber-attack.

86. The FTC recommends that identity theft victims take several costly steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone

---

[24] *See Data Breach Remediation Efforts and Their Implications for Hospital Quality*, Health Services Research https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last accessed June 7, 2022).

[25] *See, e.g.*, https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/ (last accessed September 1, 2021); https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech (last accessed on September 1, 2021).

steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, seeking a credit freeze, and correcting their credit reports.[26]

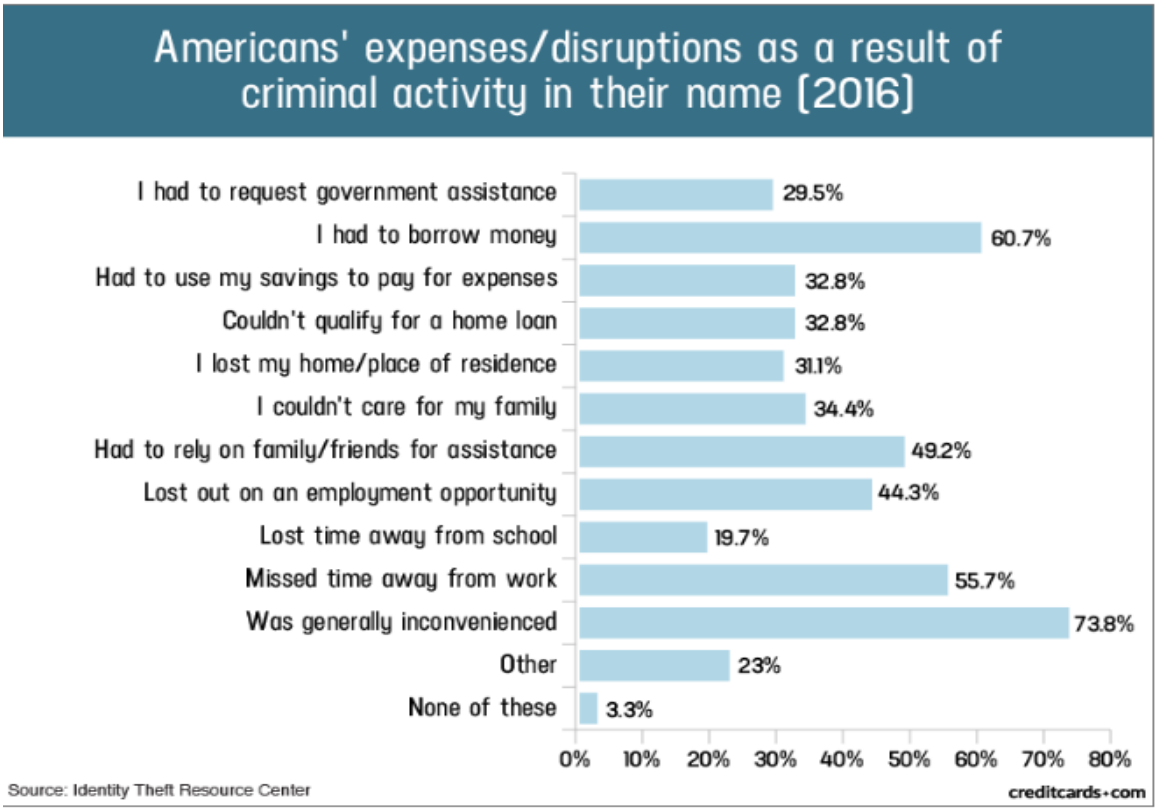
87. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

88. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

89. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest—resulting in an arrest warrant being issued in the victim's name.

90. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[27]

[26] *See* https://www.identitytheft.gov/Steps (last visited September 1, 2021).
[27] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last accessed September 1, 2021).



91. What's more, theft of Private Information is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our live become interconnected through the lens of massively complex cloud computing, PII/PHI is a valuable property right.[28]

92. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that Private Information has considerable market value.

93. Theft of PHI, in particular, is problematic because: "A thief may use your name or

[28] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[29]

94. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

95. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

96. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

97. Where the most private information belonging to Plaintiff and Class Members was accessed and removed from Defendant's network, there is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and the Class Members are at an increased risk of fraud and identity theft for many years into the future.

98. Thus, Plaintiff and the Class Members must vigilantly monitor their financial and medical accounts for many years to come.

[29] *See* Medical Identity Theft, Federal Trade Commission Consumer Information (last visited: June 7, 2022), http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

99. While credit card information can sell for as little as $1-$2 on the black market, other more sensitive information can sell for as much as $363, according to the Infosec Institute. PII is particularly valuable because criminals can use it to target victims with frauds and scams, posing as medical personnel through the use of otherwise sacrosanct information. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

100. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

101. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

102. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of

that old bad information is quickly inherited into the new Social Security number."[30]

103. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[31]

104. Medical information is especially valuable to identity thieves. The asking price on the Dark Web for medical data is $50 per person and up.[32]

105. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

106. Defendant knew or should have known this risk and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

107. Defendant's wrongful actions and/or inaction and the resulting Data Breach have placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of

[30] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited September 1, 2021).
[31] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited September 1, 2021).
[32] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last accessed September 1, 2021).

quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud." Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. There is also a high probability that criminals who now possess the Class Members' Private Information have not yet used the information but will do so at a later date or re-sell it.

108. Defendant's poor data security also deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for its service, Plaintiff and other reasonable consumers understood and expected that they were paying for both medical services and data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and the Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

109. Defendant has failed to provide adequate (or any) compensation to Class Members harmed by its negligence.

110. To date, Defendant has not offered Class Members any sort of credit monitoring and identity theft protection. Nor has it provided individual compensation for costs and burdens associated with fraudulent activity resulting from the Data Breach. Defendant has not offered the Class Members any assistance in dealing with the IRS or state tax agencies. Nor has Defendant offered to reimburse the Class Members for any costs incurred as a result of falsely filed tax returns, a common consequence of a data breach.

111. Credit monitoring services, even if Defendant eventually offers them, are also wholly inadequate in that they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud and they entirely fail to provide any compensation for the unauthorized release and disclosure

of Plaintiff's and the Class Members' Private Information.

112. Defendant breached its duty of care in negligently maintaining Plaintiff's Private Information. A reasonable person would not have shared Private Information with Defendant if they had known that it would not be secure and would be negligently maintained by Defendant.

113. Defendant has a duty to protect its patients and patients' property.

114. Defendant should have known—and perhaps had actual knowledge—that data breaches, especially health data, were on the rise and medical institutions were lucrative or likely targets of cybercriminals looking to steal PII and PHI. As mentioned above, data breaches such as the one that occurred at Defendant's business dominate headlines and should have been known to any and all medical institutions which take reasonable precautions to secure the data they maintain. Defendant owed an affirmative duty to exercise reasonable or ordinary care for the safety of the Private Information of its patients, especially given that a data breach was foreseeable. Defendant had reason to anticipate an assault on its computer system as a medical institution warehousing and storing valuable and private information of its patients.

115. Defendant voluntarily undertook the act of maintaining and storing Plaintiff's PII and PHI, and as such, the law required Defendant to do so with ordinary or reasonable care. Defendant breached its duty when it failed to implement safety and security measures sufficient to protect its patients' sensitive data from the breach that it should have anticipated.

116. To date, Defendant has done absolutely nothing to provide Plaintiff or the Class Members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time incurred because of the disruption of service at Defendant's medical facilities.

117. Plaintiff and the Class Members have been damaged by the compromise of their

Private Information in the Data Breach.

118. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

119. Plaintiff and the Class Members face a substantial risk of out-of-pocket fraud losses, such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

120. Plaintiff and the Class Members face substantial risk of being targeted in the future for phishing, data intrusion, and other illegal schemes based on their Private Information, as potential fraudsters could use exposed information to target Plaintiff and Class Members more effectively.

121. To prevent the brunt of these scams, Plaintiff and the Class Members will be forced to incur out-of-pocket costs for protective measures including but not limited to credit monitoring, credit reporting, and credit freezes directly or indirectly related to the Data Breach.

122. Plaintiff and the Class Members suffered a loss of value to their Private Information when it was acquired by cyber thieves in the Data Breach. This loss of value is real and substantive; numerous courts have recognized the propriety of loss of value in assessing damages in analogous cases.

123. Plaintiff and the Class Members were also damaged by losing the benefits of their bargains with Defendant; they overpaid for a service that was intended to be accompanied by adequate data security, but was not. Part of the price Plaintiff and the Class Members paid to Defendant was intended to fund adequate security for Defendant's computer system, ensuring the safety of Plaintiff's and the Class Members' Private Information. Plaintiff and the Class Members

did not get what they paid for.

124. Plaintiff and Class Members have spent, and will continue to spend, significant amounts of time to monitor their financial and medical accounts and records for misuse.

125. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach.

126. In addition to the losses of use and access to their medical records and the costs associated with those losses (including actual disruption of medical care and treatment), many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of the time reasonably spent in remedying and mitigating the effects of the Data Breach, including:

a. Finding alternative healthcare and treatment;

b. Delaying or foregoing healthcare and treatment;

c. Undergoing healthcare and treatment without medical providers having access to a complete medical history and records;

d. Having to retrace or recreate their medical history;

e. Finding fraudulent charges;

f. Canceling and reissuing credit and debit cards;

g. Purchasing credit monitoring and identity theft prevention;

h. Addressing their inability to withdraw funds linked to compromised accounts;

i. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

j. Placing “freezes” and “alerts” with credit reporting agencies;

k. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

l. Contacting financial institutions and closing or modifying financial accounts;

m. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

n. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

o. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

127. Moreover, Plaintiff and the Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches. This protection will only be possible if Defendant were to implement security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

128. As a result of Defendant's conduct, Plaintiff and the Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about their lives, including the ailments they suffer—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

129. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and the Class Members have suffered and will continue to suffer anxiety, emotional distress, and loss

of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

130. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

131. Plaintiff bring this action individually and on behalf of all other persons similarly situated ("the Classes") pursuant to Rule 23 of the Federal Rules of Civil Procedure ("Rule 23").

132. Plaintiff proposes the following Class definitions, subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seek certification of the following Classes:

> **National Class:** All persons whose PII and/or PHI was compromised as a result of the Data Breach of Defendant's systems from approximately March 7, 2022 to March 21, 2022 (the "National Class" or the "Class").
>
> **Massachusetts Sub-Class:** All persons in Massachusetts whose PII and/or PHI was compromised as a result of the Data Breach of Defendant's systems from approximately March 7, 2022 to March 21, 2022 (the "Massachusetts Subclass", and together with the National Class, the "Classes").

133. Excluded from the Classes are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

134. Plaintiff reserves the right to amend the definitions of the Classes or add a class or subclass if further information and discovery indicate that the definitions of the Classes should be narrowed, expanded, or otherwise modified.

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

Class Member.

136. This action satisfies the requirements for a class action under Rule 23, including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

137. Numerosity. The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Classes consists of approximately two million patients of Defendant whose data was compromised in the Data Breach.

138. Commonality and Predominance. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b) 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;

c) Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

d) Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e) Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f) Whether Defendant breached their duty to Class Members to safeguard their Private Information;

g) Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h) Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i) Whether Plaintiff and the Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j) Whether Defendant owed a duty to provide Plaintiff and Class Members notice of this data breach, and whether Defendant breached that duty;

k) Whether Defendant's conduct was negligent;

l) Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m) Whether Defendant's actions violated federal law;

n) Whether Defendant's acts violated Kentucky law, and;

o) Whether Plaintiff and the Class Members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

139. Typicality. The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff's grievances, like the proposed Class Members' grievances, all arise out of the same business practices and course of conduct by Defendant.

140. Adequacy. Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's Counsel are competent and experienced in litigating class

actions.

141. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

142. Superiority. A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with the identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined

because the Class includes only Sheild patients, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

143. In addition, Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

CAUSES OF ACTION

Count I

NEGLIGENCE

(On Behalf of Plaintiff and All Class Members)

144. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

145. Plaintiff brings this claim on behalf of himself and all members of the Classes.

146. Defendant required Plaintiff and the Class Members to submit non-public personal information in order to obtain medical services.

147. The Class Members are individuals who provided certain PII and PHI to Defendant including their names, address, date of birth, Social Security number, insurance information, medical record number, and medical information related to care received as a necessary condition of Defendant providing medical services to the Class Members.

148. Defendant had full knowledge of the sensitivity of the PII and PHI to which it was entrusted, and the types of harm that Class Members could and would suffer if the PII and PHI were wrongfully disclosed. Defendant had a duty to each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. The Class Members were the

foreseeable victims of any inadequate safety and security practices. The Class Members had no ability to protect their data in Defendant's possession.

149. By collecting and storing this data in its computer property, and by sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and the Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

150. Defendant owed a duty of care to Plaintiff and the Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

151. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as the common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

152. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

153. Some or all of the medical information at issue in this case constitutes "protected

health information" within the meaning of HIPAA.

154. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

155. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

156. Defendant breached its duties, and was negligent, by failing to use reasonable measures to protect the Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

157. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the medical industry.

158. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

159. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

160. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

Count II

BREACH OF EXPRESS CONTRACT

(On Behalf of Plaintiff and All Class Members)

161. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

162. Plaintiff brings this claim on behalf of himself and all members of the Classes.

163. Plaintiff and Class Members entered into written agreements with Defendant as part of the medical services Defendant provided to Plaintiff 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.

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

165. Defendant's failure to protect Plaintiff's and Class Members' PII and PHI constitutes a material breach of the terms of these agreements by Defendant.

166. As a direct and proximate result of Defendant's breach of contract with Plaintiff and Class Members, Plaintiff and Class Members have been irreparably harmed.

167. Accordingly, Plaintiff, individually and on behalf of the Class, respectfully requests this Court award all available damages for Defendant's breach of express contract.

Count III

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and All Class Members)

168. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

169. Plaintiff brings this claim on behalf of himself and all members of the Classes.

170. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the provision of medical care and treatment, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

171. Specifically, Plaintiff and the Class Members entered into valid and enforceable implied contracts with Defendant when they first went for medical treatment at one of Defendant's facilities.

172. The valid and enforceable implied contracts to provide medical healthcare services that Plaintiff and Class Members entered into with Defendant included Defendant's promise to

protect nonpublic Private Information given to Defendant or that Defendant created on its own from Plaintiff's and Class Members' disclosures. Plaintiff and Class Members provided this Private Information in reliance of that promise.

173. Defendant solicited and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

174. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

175. Plaintiff and Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

176. Under the implied contracts, Defendant and/or its affiliated healthcare providers promised and were obligated to: (a) provide healthcare to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Class Members agreed to pay money for these services, and to turn over their Private Information.

177. Both the provision of medical services healthcare and the protection of Plaintiff and Class Members' Private Information were material aspects of these implied contracts.

178. The implied contracts for the provision of medical services—contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's published Privacy Practices.

179. Defendant's express representations, including, but not limited to the express representations found in its Privacy Practices, memorialize and embody an implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff and Class Members' Private Information.

180. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and the Class Members, healthcare that does not adhere to industry-standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

181. A meeting of the minds occurred when Plaintiff and the Class Members agreed to, and did, provide their Private Information to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, (a) the provision of healthcare and medical services and (b) the protection of their Private Information.

182. Plaintiff and the Class Members performed their obligations under the contract when they paid for their healthcare services and provided their Private Information.

183. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

184. Defendant materially breached the terms of its implied contracts, including, but not limited to, the terms stated in the relevant Privacy Practices. Defendant did not maintain the privacy of Plaintiff's and the Class Members' Private Information as evidenced by its late notification of the Data Breach to Plaintiff and approximately two million Class Members. Specifically, Defendant did not comply with industry standards, the standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

185. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

186. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains, and instead received healthcare and other services that were of a diminished value compared to those described in the contracts. Plaintiff and Class Members were therefore 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.

187. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

188. As a direct and proximate result of the Data Breach, Plaintiff and the Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including, without limitation, the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in

the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

189. Plaintiff and the Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

190. Plaintiff and the Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

Count IV

INVASION OF PRIVACY BY INTRUSION

(On Behalf of Plaintiff and All Class Members)

191. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

192. Plaintiff brings this claim on behalf of himself and all members of the Classes.

193. Plaintiff and the Classes had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

194. Defendant owed a duty to its current and former patients, including Plaintiff and the Class Members, to keep their Private Information contained as a part thereof, confidential.

195. Defendant failed to protect and released to unknown and unauthorized third parties the Private Information of Plaintiff and the Class Members.

196. Defendant allowed unauthorized and unknown third parties access to and examination of the Private Information of Plaintiff and the Class Members, by way of Defendant's failure to protect the Private Information.

197. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and the Class Members is highly offensive to a reasonable person.

198. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class Members disclosed their Private Information to Defendant as part of the current and former patients' medical treatment with Defendant, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

199. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

200. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its information security practices were inadequate and insufficient.

201. Defendant acted with reckless disregard for Plaintiff's and Class Members' privacy when it allowed improper access to its systems containing Plaintiff's and Class Members' Private Information.

202. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' data.

203. Because Defendant acted with this knowing state of mind, they had notice and knew

the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class Members.

204. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiff and the Class Members was disclosed to third parties without authorization, causing Plaintiff and the Class Members to suffer damages.

205. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class Members.

Count V

BREACH OF FIDUCIARY DUTY

(On Behalf of Plaintiff and All Class Members)

206. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

207. Plaintiff brings this claim on behalf of himself and all members of the Classes.

208. In providing their Private Information to Defendant, Plaintiff and Class Members justifiably placed special confidence in Defendant to act in good faith and with due regard to the interests of Plaintiff and Class Members in order to safeguard and keep confidential that Private Information.

209. Defendant accepted the special confidence placed in it by Plaintiff and Class Members, as evidenced by its assertion 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 Plaintiff and Class Members in preserving the confidentiality of the Private Information.

210. In light of the special relationship between Defendant, Plaintiff, and the Class Members, whereby Defendant became the guardian of Plaintiff's and the Class Members' Private Information, Defendant accepted a fiduciary duty to act primarily for the benefit of its patients, including Plaintiff and the Class Members. This duty included safeguarding Plaintiff's and the Class Members' Private Information.

211. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its medical relationship with its patients, in particular, to keep secure the Private Information of those patients.

212. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, or give notice of the Data Breach in a reasonable and practicable period of time.

213. Defendant breached its fiduciary duties to Plaintiff and the Class Members by failing to encrypt and otherwise protect the integrity of its computer systems containing Plaintiff's and the Class Members' Private Information.

214. Defendant breached the fiduciary duties it owed to Plaintiff and the Class Members by failing to timely notify and/or warn them of the Data Breach.

215. Defendant breached its fiduciary duties by failing to 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).

216. Defendant breached its fiduciary duties by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access

only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1).

217. Defendant breached its fiduciary duties by 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).

218. Defendant breached its fiduciary duties by failing to 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).

219. Defendant breached its fiduciary duties by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. § 164.306(a)(2).

220. Defendant breached its fiduciary duties by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3).

221. Defendant breached its fiduciary duties by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(94).

222. Defendant breached its fiduciary duties by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. § 164.502, *et seq.*

223. Defendant breached its fiduciary duties by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures necessary to maintain the security of PHI, in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

224. Defendant breached its fiduciary duties by failing to 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).

225. Defendant breached its fiduciary duties by otherwise failing to safeguard Plaintiff's and the Class Members' Private Information.

226. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the 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 Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

227. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff 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 VI

BREACH OF CONFIDENCE

(On Behalf of Plaintiff and All Class Members)

228. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

229. Plaintiff brings this claim on behalf of himself and all members of the Classes.

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

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

232. Plaintiff and the Class Members receiving treatment from Defendant provided Plaintiff's 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.

233. Plaintiff and the Class Members receiving treatment from Defendant also provided Plaintiff's 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.

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

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

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

237. But for Defendant's disclosure of Plaintiff's and the Class Members' Private Information in violation of the parties' understanding of confidence, their PII 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 Plaintiff's and the Class Members' Private Information as well as the resulting damages.

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

239. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class Members, Plaintiff and the Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and

attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of current and former patients; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

240. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff 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 VII

VIOLATION OF MASSACHUSETTS GENERAL LAWS CHAPTER 214 § 1B

(On Behalf of Plaintiff and the Massachusetts Sub-Class Members)

241. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

242. Plaintiff brings this claim on behalf of himself and all members of the Massachusetts Sub-Class.

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

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

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

246. Plaintiff's and Class Members' Private Information was accessed in an unauthorized manner while in the custody of Defendant.

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

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

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

250. The acts an omissions of Defendant described above constitute a violation of Mass. Gen. L. c 214 § 1B.

251. As a direct and proximate result of Defendant's deceptive acts or practices, Plaintiff and Massachusetts Sub-Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have sought medical services from Defendant but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Private Information; and an increased, imminent risk of fraud and identity theft.

252. Defendant's violations present a continuing risk to Plaintiff and Massachusetts Sub-Class Members as well as to the general public.

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

Count VIII

UNJUST ENRICHMENT

(On Behalf of Plaintiff and All Class Members)

254. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

255. Plaintiff hereby pleads this Count in the alternative to Counts II and III.

256. Plaintiff and Class Members conferred a monetary benefit on Defendant.

257. Defendant received and retained money belonging to Plaintiff and the Class.

258. Defendant appreciates or has knowledge of such benefit.

259. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, which Defendant has unjustly received as a result of its unlawful actions.

260. As a result of Defendant's conduct, Plaintiff and Class Members suffered and will continue to suffer actual damages including, but not limited to, the release of their Private Information; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; and time spent initiating fraud alerts. Plaintiff and Class Members suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, other economic and noneconomic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Classes;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims in this Complaint so triable. Plaintiff also respectfully request leave to amend this Complaint to conform to the evidence, if such amendment is needed for trial.

Dated: June 9, 2022

Respectfully Submitted,

/s/ Jonathan T. Merrigan
J. Tucker Merrigan, BBO# 681627
Peter M. Merrigan, BBO# 673272
SWEENEY MERRIGAN LAW, LLP
268 Summer Street, LL
Boston, MA 02210
Tel: (617) 391-9001
Fax: (617) 357-9001
tucker@sweeneymerrigan.com
peter@sweeneymerrigan.com

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

Todd. S. Garber (*pro hac vice* forthcoming)
Andrew White (*pro hac vice* forthcoming)
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel: (914) 298-3281
Fax: (914) 824-1561
tgarber@fbfglaw.com
awhite@fbfglaw.com

Attorneys for Plaintiff and the Putative Classes