UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ELSIE DIAZ, individually and on behalf of themselves and all others similarly situated, Plaintiff, v. SHIELDS HEALTH CARE GROUP, INC., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff ELSIE DIAZ ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint for Damages against Defendant Shields Health Care Group, Inc. ("Defendant" or "Shields") and hereby alleges upon personal knowledge as to her own actions, and upon information and belief and the investigation of counsel as to all other matters, as follows:

I. NATURE OF THE CASE

1. Defendant Shields is a health-care provider that provides "high-field open-bore MRI machines" and "provides other MRI, PET/CT and ambulatory surgery services to patients at more than 30 locations in New England."[1]

2. As part of the services Shields provides, Shields requires patients to provide personally identifiable information ("PII"), including full name, address, date of birth, and Social

[1] https://shields.com, (last accessed June 12, 2022)).

Security number, as well as protected health information ("PHI"), including provider information, diagnosis, billing information, insurance number and information, medical record number(s) patient ID, and other medical or treatment information (collectively, "Private Information").

3. Between the dates of March 7, 2022 and March 21, 2022, an unauthorized individual or individuals acquired "certain data" from the computer systems and network of Defendant and/or its agents.[2] The Notice of Data Security Incident (hereinafter, the "Notice"), however, is unclear – it states that Shields became aware of suspicious activity on March 28, 2022, while the Notice also states that Shields "had identified a security alert on or around March 18, 2022," which is when the Data Breach was actively occurring. Either way, Shields did not post a notice regarding the Data Breach until June of 2022 – months after it first became clear that a data incident or breach had occurred with respect to Shields' network of providers (who were also affected).[3]

4. The Notice states "*Shields takes the confidentiality privacy and security of information in our care seriously*," while it also omits the following critical information: (i) when Defendant first knew precisely of the Data Breach; (ii) specifically what information was accessed or acquired specific to Plaintiff and the Class Members (the Notice only lists the Private Information and says what was compromised "could include one or more of the following"; and, (iii) how Defendant's servers were compromised.

5. Defendant also failed to notify consumers for two full months from when their investigation was complete, waiting from March of 2022 to June of 2022 until the Notice was posted on its website. Further, if Defendant had been monitoring its servers for the presence of

[2] https://shields.com/notice-of-data-security-incident/, (last accessed June 12, 2022)(hereinafter, "Notice").
[3] The list of providers affected is included in the "Factual Allegations" portion of this Complaint, under "Defendant's Business."

hackers, malware, ransomware, or whatever type of cyberattack occurred here (Plaintiff and the Class Members have no way of knowing because the Notice does not provide this information), Defendant would have detected the presence of the unauthorized individual(s) sooner. When considering the value of the Private Information at stake, and the proclivity of this Private Information to end up being sold to criminals on the dark web (as that is the *modus operandi* of a targeted hacking effort such as this Data Breach), every second that passes is critical to the victims' efforts in mitigating risk and the harm caused by Defendant. Waiting months before informing Plaintiff and Class Members of their data being compromised compounds the harm caused by the Data Breach itself.

6. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect patients' Private Information.

7. Plaintiff brings this class action lawsuit on behalf of those current or former patients of Defendant who are similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party.

8. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks.

9. Upon information and belief, the mechanism of the hacking and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to

Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

10. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard patient Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members prompt notice of the Data Breach.

11. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner, as opposed to letting cyberthieves roam freely in Defendant's IT network for two full weeks.

12. 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. This present risk will continue for their respective lifetimes.

13. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, 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' 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.

14. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a substantial and present 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.

15. Plaintiff and Class Members will incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

16. Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

17. Plaintiff seeks remedies including, but not limited to, damages, restitution, and injunctive relief, as well as reasonable attorneys' fees and costs, on behalf of themselves and the Class.

II. JURISDICTION AND VENUE

18. This Court has jurisdiction over the subject matter of this Action pursuant to the Class Action Fairness Act: minimal diversity exists as Defendant and members of the Class are residents of different states; there are at least 100 members of the putative Class, as there are nearly 2,000,000 impacted victims, and the amount-in-controversy aggregated across the Plaintiff's losses and that of the Class exceed $5,000,000 exclusive of costs and interest.

19. Personal jurisdiction exists over the Defendant because Defendant sells its services in Massachusetts, it is headquartered in Massachusetts, it does business in Massachusetts, and it is a corporation registered in Massachusetts.

20. Venue is proper in the District of Massachusetts because Defendant is headquartered here, and because a substantial part of the events or omissions giving rise to the

claim occurred, or a substantial part of property that is the subject of the action is situated in this District.

III. PARTIES

Plaintiff

21. Plaintiff Elsie Diaz is a resident of the state of Massachusetts who resides in Weymouth, Massachusetts. Plaintiff has been a patient of the Defendant for approximately twenty-nine years and on multiple occasions has been required to provide her Private Information. In addition, to the damages detailed herein, Plaintiff is now subject to the present and continuing risk of identity theft and fraud, and must spend hours of her time carrying out the extensive set of steps Defendant advised that consumers should take to protect themselves.

Defendant Shields Health Care Group, Inc.

22. 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.

IV. FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

23. Defendant Shields is a health-care provider that provides "high-field open-bore MRI machines" and "provides other MRI, PET/CT and ambulatory surgery services to patients at more than 30 locations in New England."[4]

24. Pursuant to the Notice, the following providers within the Shields Health Care Group had patients who were impacted by the Data Breach[5]:

Baystate Health Urgent Care, LLC
Baystate MRI & Imaging Center, LLC

[4] https://shields.com, (last accessed June 12, 2022)).
[5] https://shields.com/notice-of-data-security-incident/, (last accessed June 12, 2022).

Brighton Imaging Center, LLC
Cape Cod CT Services, LLC
Cape Cod Imaging Services, LLC (a business associate to Falmouth Hospital Association, Inc)
Cape Cod PET/CT Services, LLC
Cape Cod Radiation Therapy Service, LLC
Central Maine Medical Center
Emerson Hospital
Fall River/New Bedford Regional MRI Limited Partnership
Falmouth Hospital Association, Inc.
Franklin MRI Center, LLC
Lahey Clinic MRI Services, LLC
Massachusetts Bay MRI Limited Partnership
Mercy Imaging, Inc.
MRI/CT of Providence, LLC
Newton-Wellesley MRI Limited Partnership
NW Imaging Management Company, LLC (a business associate to Newton Wellesley Orthopedic Associates, Inc.)
Newton-Wellesley Imaging, PC
Newton Wellesley Orthopedic Associates, Inc.
Northern MASS MRI Services, Inc.
PET-CT Services by Tufts Medical Center and Shields, LLC
Shields and Sports Medicine Atlantic Imaging Management Co, LLC (a business associate SportsMedicine Atlantic Orthopaedics P.A.)
Shields CT of Brockton, LLC
Shields Imaging at Anna Jaques Hospital, LLC
Shields Healthcare of Cambridge, Inc.
Shields Imaging at University Hospital, LLC
Shields Imaging at York Hospital, LLC
Shields Imaging Management at Emerson Hospital, LLC (a business associate to Emerson Hospital)
Shields Imaging of Eastern Mass, LLC
Shields Imaging of Lowell General Hospital, LLC
Shields Imaging of Portsmouth, LLC
Shields Imaging with Central Maine Health, LLC (a business associate to Central Maine Medical Center)
Shields Management Company, Inc.
Shields MRI & Imaging Center of Cape Cod, LLC
Shields MRI of Framingham, LLC
Shields PET/CT at CMMC, LLC
Shields PET_CT at Berkshire Medical Center, LLC
Shields PET-CT at Cooley Dickinson Hospital, LLC
Shields PET-CT at Emerson Hospital, LLC
Shields Radiology Associates, PC

Shields Signature Imaging, LLC
Shields Sturdy PET-CT, LLC
Shields-Tufts Medical Center Imaging Management, LLC (a business associate to Tufts Medical Center, Inc.)
South Shore Regional MRI Limited Partnership
Southeastern Massachusetts Regional MRI Limited Partnership
SportsMedicine Atlantic Orthopaedics P.A.
Tufts Medical Center, Inc.
UMass Memorial HealthAlliance MRI Center, LLC
UMass Memorial MRI – Marlborough, LLC
UMass Memorial MRI & Imaging Center, LLC
Winchester Hospital / Shields MRI, LLC
Radiation Therapy of Southeastern Massachusetts, LLC
Radiation Therapy of Winchester, LLC
South Suburban Oncology Center Limited Partnership
Shields Imaging of North Shore, LLC

25. In the ordinary course of receiving treatment and healthcare services from Defendant, patients are required to provide sensitive, private information, including full name, address, date of birth, and Social Security number provider information, diagnosis, billing information, insurance number and information, medical record number(s) patient ID, and other medical or treatment information.

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

27. As a condition of receiving medical care and treatment at Defendant's facilities, Defendant requires that its patients entrust it with highly sensitive personal information.

28. On information and belief, Defendant made promises and representations to its patients, including Plaintiff and Class Members, that the PHI and PII collected from them as a condition of utilizing Defendant's services and/or employment would be kept safe, confidential, and that the privacy of that information would be maintained.

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

30. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

31. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

THE DATA BREACH

32. On an unspecified date, which is omitted from the Notice, between March of 2022 and June of 2022, the Defendant determined that an "unknown actor gained access to certain Shields systems from March 7, 2022 to March 21, 2022 [… f]urthermore, the investigation revealed that certain data was acquired by the unknown actor within that time frame."[6]

33. As the Notice states, "[the type of information that was or may have been impacted could include one or more of the following: [f]ull name, Social Security number, date of birth, home address, provider information, diagnosis, billing information, insurance number and information, medical record number, patient ID, and other or treatment information."[7]

34. Upon information and belief, the unauthorized individuals did in fact access Defendant's files, and exfiltrate the Private Information of patients during the approximately nine days that those unauthorized individuals had unfettered access to Defendant's network.

---

[6] https://shields.com/notice-of-data-security-incident/, (last accessed June 12, 2022).
[7] *Id.*

35. Upon information and belief, the Private Information contained in the files accessed by the unauthorized individuals was not encrypted.

36. Defendant failed to immediately begin notifying victims of the Data Breach – waiting approximately two months (June of 2022) until the Notice was posted on Defendant's website.

37. Due to Defendant's incompetent and ineffective security measures, Plaintiff and the Class Members now face a present and substantial risk of fraud and identity theft and must deal with that threat forever.

38. Plaintiff believes her Private Information was stolen in the Data Breach and that said information was subsequently posted for sale on the dark web, as that is the *modus operandi* of all cybercriminals.

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

40. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

41. Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

42. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[8] Of the 1,473 recorded

[8] 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 1, 2021).

data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[9] The 525 reported 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.[10]

43. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including, American Medical Collection Agency (25 million patients, March 2019) University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

44. In 2021 alone there were over 220 data breach incidents.[11] These approximately 220 data breach incidents have impacted nearly 15 million individuals.[12]

45. Indeed, cyberattacks 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."[13]

---

[9] *Id*.
[10] *Id* at 15.
[11] *See* Kim Delmonico, Another (!) Orthopedic Practice Reports Data Breach, Orthopedics This Week (May 24, 2021), https://ryortho.com/breaking/another-orthopedic-practice-reports-data-breach/.
[12] *Id*.
[13] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited July 2, 2021).

46. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[14]

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

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

48. 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.

49. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient 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.[15] 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.[16]

50. 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

---

[14] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

[15] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 15, 2021).

[16] *Id*.

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.

51. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient 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. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

52. 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.")

53. Defendant failed to properly implement basic data security practices.

54. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

55. 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

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

57. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

58. Other best cybersecurity 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 protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

59. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

60. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

DEFENDANT'S CONDUCT VIOLATES HIPAA and HITECH AND EVIDENCES ITS INSUFFICIENT DATA SECURITY

61. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

62. Defendant is a covered entity pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

63. Defendant is a covered entity pursuant to the Health Information Technology Act ("HITECH")[17]. *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

64. The HIPAA and HITECH rules work in conjunction with the already established laws of privacy Massachusetts. HIPAA and HITECH do not recognize an individual right of claim for violation but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

65. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

66. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. See 42 C.F.R. §§ 164.302-164.318.

[17] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

67. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart. *See* 45 C.F.R. § 164.530(c).

68. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

69. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

70. Under HIPAA:

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.[18]

[18] 45 C.F.R. § 160.103

71. HIPAA and HITECH obligated Defendant to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. §17902.

72. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

73. HIPAA further obligated Defendant to ensure that its workforce complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train its workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

74. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance

Material.[19] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[20]

75. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

> (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);
>
> (2) the recipient of the PHI;
>
> (3) whether the PHI was actually acquired or viewed; and
>
> (4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[21]

76. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

---

[19] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
[20] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
[21] 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304

77. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train its employees and staff so that all its staff and employees know their roles in facility security.

78. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

79. Had Plaintiff and the Class Members known Defendant would not honor its own policies and procedures and abide by the federal rules and regulations of privacy they would not have provided their PHI to Defendant and sought treatment elsewhere.

80. 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 PII 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).

81. A Data Breach cyberattack such as the one Defendant experienced, is considered a breach under the HIPAA Rules 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

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

DEFENDANT'S BREACH

83. Defendant breached its obligations to Plaintiff and Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems 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, cyber-attacks, hacking incidents, and ransomware attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing or prior intrusions;

d. 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);

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

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

g. 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);

h. 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);

i. 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);

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

k. 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);

l. 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's definition of "encryption");

m. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

n. Failing to adhere to industry standards for cybersecurity.

84. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

85. Accordingly, as outlined below, Plaintiff and Class Members now face a present,

increased, and immediate risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

CYBERTATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTITY THEFT

86. Hacking incidents and data breaches at medical facilities like Defendant's facilities are especially problematic because of the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

87. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[22]

88. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[23]

89. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[24]

90. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black

---

[22] *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.

[23] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[24] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

91. The FTC recommends that identity theft victims take several 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 steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[25]

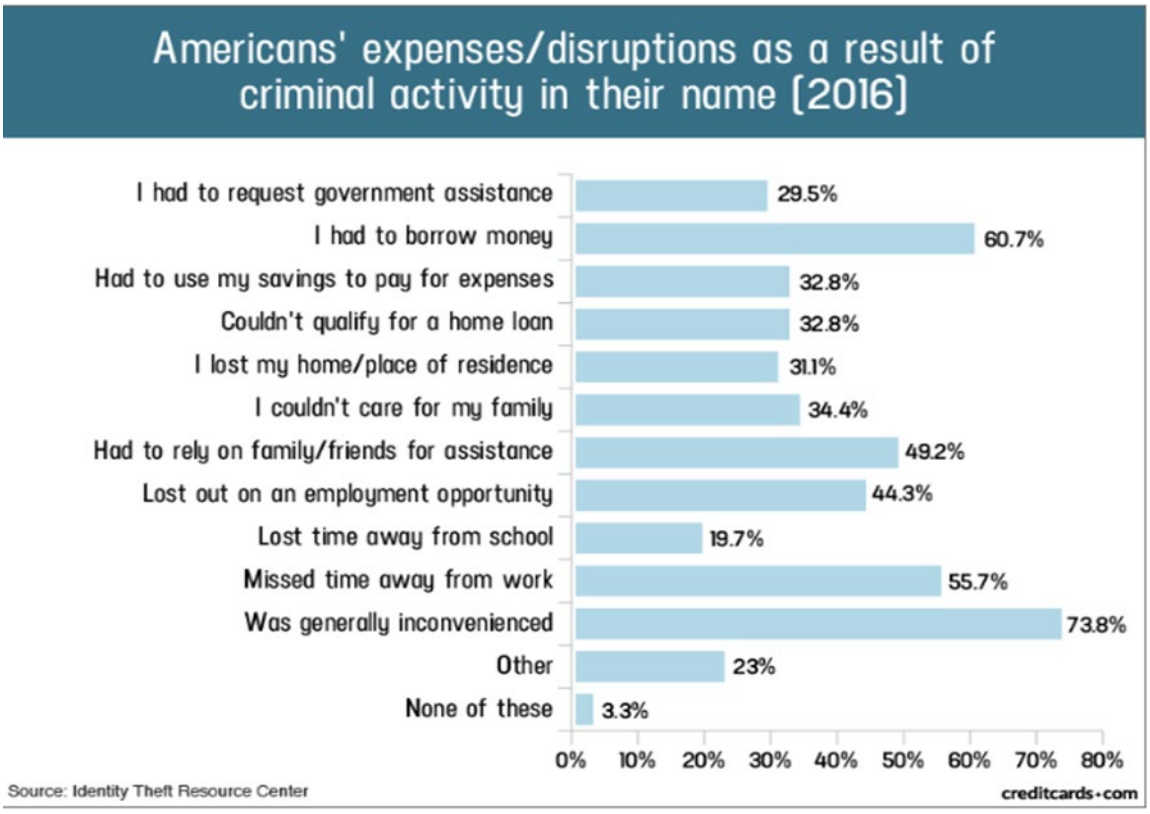
92. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

93. 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. In addition, identity thieves may obtain a job using the victim's Social

[25] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Mar. 16, 2021).

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.

94. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[26]



95. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.[27]

96. Its value is axiomatic, considering the value of "big data" in corporate America and

[26] *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.

[27] *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).

the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

97. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or 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."[28]

98. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and 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.

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

100. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at p. 29.

[28] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Mar. 16, 2021).

101. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

102. 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 Class Members are at an increased risk of fraud and identity theft for many years into the future.

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

104. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[29] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

105. 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.[30] 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.[31] 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

---

[29] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[30] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 16, 2021).

[31] *Id* at 4.

individual's authentic tax return is rejected.

106. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

107. 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."[32]

108. 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."[33]

109. Medical information is especially valuable to identity thieves.

110. According to account monitoring company LogDog, medical data was selling for $50 and up on the Dark Web.[34]

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

112. For this reason, Defendant knew or should have known about these dangers and strengthened its network and data security 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

---

[32] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[33] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[34] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

that risk.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

113. To date, Defendant has done less than nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach. Defendant's data breach Notice completely downplays and disavows the theft of Plaintiff and Class Members Private Information, when the facts demonstrate that the Private Information was accessed and exfiltrated. There was no identity theft or credit monitoring offered by the Defendant by way of the Notice that was posted online. Identity theft or credit monitoring is the bare minimum that a Defendant can offer after a data breach such as the Data Breach alleged herein.

114. Plaintiff and Class Members have been injured and damaged by the compromise of their Private Information in the Data Breach.

115. On information and belief, Plaintiff's Private Information was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendant's IT network. Class Members' PII and PHI, as described above, was similarly compromised and is now in the hands of the same cyberthieves.

116. Plaintiff is a patient of Defendant.

117. Plaintiff typically takes measures to protect her Private Information, and is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

118. Plaintiff stores any documents containing her PII and PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her online accounts.

119. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff has spent five to six hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. Moreover, this time was spent at Defendant's direction. Defendant's Notice of Data Security Incident expressly advised Plaintiff to spend time mitigating her damages, including, for example, "monitor [your] accounts."[35]

120. As a result of the Data Breach, Plaintiff has suffered anxiety as a result of the release of their Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

121. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from identity theft and fraud.

[35] https://shields.com/notice-of-data-security-incident/, (last accessed June 12, 2022).

122. Indeed, Plaintiff experienced fraudulent activity on her debit card shortly after the data beach. On or about March 11, 2022, a fraudulent transaction was attempted in the amount of $40.68 at an East Boston Pizza Shuttle restaurant.

123. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

124. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical fraud, insurance fraud, tax return fraud, utility bills opened in their names, and similar identity theft.

125. Defendant has admitted Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

126. Plaintiff and Class Members will also incur out-of-pocket costs for protective measures such as credit monitoring fees (for any credit monitoring obtained in addition to or in lieu of the inadequate monitoring offered by Defendant), credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

127. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by the hacker and cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

128. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied

by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for.

129. 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.

130. Plaintiff and Class Members have suffered actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

i. Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;

ii. Purchasing credit monitoring and identity theft prevention;

iii. Placing "freezes" and "alerts" with credit reporting agencies;

iv. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

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

vi. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

131. Moreover, Plaintiff and 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 by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing sensitive and confidential personal, health, and/or financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

132. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

133. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at a present, imminent and increased risk of future harm.

V. CLASS ALLEGATIONS

134. Plaintiff brings this class action as a class action on behalf of themselves and the following similarly situated persons:

> **Class Definition.** All persons whose Private Information was compromised in the Data Breach and were sent a notice of the Data Breach from the Defendant.

Excluded from the Class' 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 Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

135. Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

136. **Numerosity.** On information and belief, the putative Class is comprised of millions of individuals making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

137. **Commonality.** Questions of law and fact common to all Class Members exist and predominate over questions affecting individual Class Members, including, *inter alia*:

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 hacking incident and Data Breach;

c. Whether Defendant's data security systems prior to and during the hacking incident and Data Breach complied with applicable data security laws and regulations, *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 its 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 Defendant owed a duty to provide Plaintiff and Class Members notice of this Data Breach, and whether Defendant breached that duty to provide timely notice;

j. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct was *per se* negligent;

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

n. Whether Defendant was unjustly enriched;

o. Whether Defendant's conduct violated federal law;

p. Whether Defendant's conduct violated state law;

q. Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or punitive damages.

138. **Adequacy of Representation.** Plaintiff and their counsel will fairly and adequately represent the interests of the other Class Members. Plaintiff has no interests antagonistic to, or in conflict with, the other Class Members' interests. Plaintiff's counsel is highly experienced in the prosecution of consumer class action data breach cases.

139. **Typicality.** Plaintiff's claims are typical of the other Class Members' claims that Plaintiff's claims and the other Class Members' claims all arise from Defendant's failure to properly safeguard and protect their Private Information.

140. **Predominance.** Defendant have 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 system 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.

141. **Superiority.** A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiff's and other Class Members' claims. Plaintiff and the other Class Members have been harmed as a result of Defendant's wrongful actions and/or inaction and the resulting breach. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct.

142. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights. Absent a class action. Defendant will retain the benefits of its wrongdoing despite serious violations of the law.

VI. CAUSES OF ACTION

COUNT I

NEGLIGENCE

143. Plaintiff re-alleges and incorporates by reference all previous paragraphs as if fully set forth herein. Plaintiff brings this claim individually and on behalf of all Class Members.

144. In order to receive medical treatments and services, Defendant and/or its agents required Plaintiff and Class Members to submit non-public Private Information, such as PII and PHI.

145. Plaintiff and Class Members entrusted their Private Information to Defendant and/or its agents with the understanding that Defendant would safeguard their information.

146. By collecting and storing this data in its computer property, and 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 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.

147. Defendant owed a duty of care to safeguard the Private Information of Plaintiff and Class Members in its custody. This duty of care arises because Defendant knew of a foreseeable risk to the data security systems it used. Defendant knew of this foreseeable risk because of the explosion of data breach incidents involving healthcare providers detailed above. Despite its knowledge of this foreseeable risk, Defendant failed to implement reasonable security measures.

148. Defendant owed a duty of care to Plaintiff and 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.

149. 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 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.

150. 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©(1).

151. Some or all of the information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

152. 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.

153. 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.

154. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect 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 their networks and systems;

c. Failure to periodically ensure that their 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 regarding what type of Private Information had been compromised 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 data breach.

155. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of hacking incidents, cyberattacks, and data breaches in the healthcare industry.

156. 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.

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

COUNT II

BREACH OF IMPLIED CONTRACT

158. Plaintiff re-alleges and incorporates by reference all previous paragraphs as if fully set forth herein. Plaintiff brings this claim individually and on behalf of all Class Members.

159. 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 Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

160. 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.

161. Defendant manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiff's and Class Members' Private Information.

162. The valid and enforceable implied contracts to provide medical health care services that Plaintiff's and Class Members entered into with Defendant and/or its Agents include the promise to protect non-public Private Information given to Defendant or that Defendant creates on its own from disclosure.

163. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for medical services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

164. 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.

165. 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.

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

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

168. On information and belief, 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 believed to be acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice (or other privacy policy-type document).

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

170. Consumers of healthcare value their privacy and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiff and 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.

171. Plaintiff and Class Members would not have entrusted their Private Information to Defendant and/or its agents 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.

172. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant and/or its agents, and paid for the provided healthcare in exchange for, amongst other things, both the provision of health care and medical services and the protection of their Private Information.

173. Plaintiff and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

174. Defendant materially breached its contractual obligation to protect the non-public Private Information Defendant gathered when the sensitive information was accessed by unauthorized personnel as part of the hacking incident and Data Breach.

175. Defendant materially breached the terms of the implied contracts. Defendant did not maintain the privacy of Plaintiff and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and hundreds, if not thousands, of Class Members. In particular, Defendant did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiff and the Class Members' Private Information, as set forth above.

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

177. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received health-care and other medical services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the health care they received.

178. 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.

179. As a direct and proximate result of the Data Breach, Plaintiff and 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, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

180. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the hacking incident and Data Breach.

COUNT III

BREACH OF FIDUCIARY DUTY

181. Plaintiff re-alleges and incorporates by reference all of the preceding paragraphs as if fully set forth herein. Plaintiff brings this claim individually and on behalf of all Class Members.

182. 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.

183. 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.

184. 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.

185. 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.

186. 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.

187. 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.

188. 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.

189. 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).

190. 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).

191. 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).

192. 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).

193. 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).

194. 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).

195. 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).

196. 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.*

197. 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).

198. 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).

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

200. 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.

201. 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 IV

UNJUST ENRICHMENT

(Alternatively to Count II)

202. Plaintiff re-alleges and incorporates by reference all of the preceding paragraphs as if fully set forth herein. Plaintiff brings this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of implied contract count above.

203. Plaintiff and Class Members conferred a benefit on Defendant with their money or labor services. Specifically, they purchased goods and services from Defendant and/or provided their labor and in so doing also provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

204. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

205. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

206. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

207. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

208. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

209. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

210. Plaintiff and Class Members have no adequate remedy at law.

211. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts 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; (f) 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 Private Information in their

continued possession; and (g) 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 Class Members.

212. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

213. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on their own and behalf of all others similarly situated, pray for relief as follows:

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

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

C. For an award of damages, restitution, and injunctive relief, as well as reasonable attorneys' fees and costs, on behalf of themselves and the Class.

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

E. For injunctive and other equitable relief to ensure the protection of the sensitive information of Plaintiff and the class which remains in Defendant's possession.

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

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

H. Such other and further relief as the Court may deem just and proper.

VIII. JURY TRIAL DEMAND

214. Plaintiff hereby demands a trial by jury of all claims so triable.

DATE: June 24, 2022

Respectfully submitted,

/s/ *Randi Kassan*

Randi Kassan
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza
Garden City, NY 11530
Telephone: (212) 594-5300
rkassan@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street
Suite 2100
Chicago, IL 60606
Tel.: (866) 252-0878
Email: gklinger@milberg.com

Samuel J. Strauss
Raina C. Borrelli
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com

ATTORNEYS FOR PLAINTIFF

pro hac vice forthcoming