UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF VERMONT

PATRICIA MARSHALL, on behalf of herself and all others similarly situated,
Plaintiff

v.

LAMOILLE HEALTH PARTNERS, INC.,
Defendant

Case No. 2:22-CV-166

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Patricia Marshall ("Plaintiff") brings this Class Action Complaint against Lamoille Health Partners, Inc. ("LHP" or "Defendant"), as an individual and on behalf of all others similarly situated, makes the following allegations upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, and those facts that are a matter of public record.

Nature of Action

1. This class action arises out of the recent targeted cyberattack against Defendant LHP, an integrated healthcare provider located in Morrisville, Vermont, that allowed a third party to access Defendant LHP's computer systems and data, resulting in the compromise of highly sensitive personal information belonging to thousands of current and former patients of LHP (the "Data Breach"). Because of the Data Breach, Plaintiff and more than 59,381[1] other victims ("Class Members") suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited August 24, 2022).

gravel & shea
76 St. Paul Street
Post Office Box 369
Burlington, Vermont 05402-0369

of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their sensitive personal information.

2. Information compromised in the Data Breach includes names, addresses, dates of birth, Social Security numbers, patient identification numbers, account numbers, financial information, health insurance information, medical information, and other protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and additional personally identifiable information ("PII") that Defendant collected and maintained (collectively the "Private Information").

3. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their Private Information had been subject to the unauthorized access of an unknown third party or precisely what specific type of information was accessed.

4. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to a cyberattack. Upon information and belief, the mechanism of the Data Breach 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.

5. In addition, Defendant and its employees failed to properly monitor the computer network and IT systems that housed the Private Information.

6. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that LHP collected and maintained is now in the hands of data thieves.

7. 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' 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.

8. As a 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.

9. By the Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

10. 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 services funded by Defendant.

11. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) breach of implied contract; (iii) breach of fiduciary duty; and (iv) unjust enrichment.

Parties

12. Plaintiff Patricia Marshall is a resident and citizen of Vermont, residing in Saint Albans, Vermont. Ms. Marshall received a letter, dated August 10, 2022 by U.S. Mail, from Defendant's Chief Executive Officer Stuart May, informing her that her Personal Information, stored on Defendant's computer systems, may have been accessed and acquired by unauthorized third parties (the "Data Breach Letter").

13. Defendant Lamoille Health Partners, Inc., is a Vermont non-profit corporation with its principal place of business at 609 Washington Highway, Morrisville, Vermont 05661.

14. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

15. All of Plaintiff's claims stated herein are asserted against LHP and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

Jurisdiction and Venue

16. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than one hundred putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendant.

17. The District of Vermont has personal jurisdiction over Defendant because Defendant is incorporated and has its principal place of business in this District; conducts

substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant's principal place of business is in this District.

Facts

Defendant's Business

19. Defendant is a health care institution that provides health care, dentistry, and pharmacy services in the State of Vermont. Defendant has approximately six treatment locations with offices in Vermont. Defendant offers medical and dental services and clinics in the fields of family medicine, pediatrics, dentistry, and behavioral health and wellness.

20. In the ordinary course of receiving healthcare care services from Defendant each patient must provide (and Plaintiff did provide) Defendant with sensitive, personal, and private information, such as their:

a. Name, address, phone number, and email address;

b. Date of birth;

c. Social Security number;

d. Demographic information;

e. Driver's license or state or federal identification;

f. Information relating to the individual's medical history;

g. Insurance information and coverage; and

h. Banking and/or credit card information.

21. Defendant also creates and stores medical records and other protected health information for its patients, including records of treatments and diagnoses.

22. Upon information and belief, LHP's HIPAA Privacy Policy is provided to every patient prior to receiving treatment and is also available upon request.

23. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws, including HIPAA.

24. The patient information held by Defendant LHP in its computer system and network included the Private Information of Plaintiff and Class Members.

25. 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.

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

27. Plaintiff and 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 Cyberattck

28. On or around August 10, 2022, LHP first began notifying Class Members and state Attorney Generals ("AGs") about a widespread data breach of its computer systems and involving the sensitive personal identifiable information of certain persons.[2]

29. Plaintiff and Class Members in this action were, upon information and belief, former and current patients of LHP.

30. The first time that Plaintiff and Class Members learned of the Data Breach was when they received by U.S. Mail Notice of Data Breach letters dated August 10, 2022, directly from LHP.

31. According to its Notice Letters, LHP explained that it discovered June 13, 2022 that "an unknown, unauthorized third party locked some of our files in a ransomware attack."[3]

32. LHP explained that a ransomware attack occurs when a "criminal deploys malicious software to lock an organization's files until the organization pays a ransom or restores their data from backups."[4]

33. After conducting an investigation into the incident LHP admitted that "an unauthorized third party may have accessed certain documents from our systems between June 12, 2022 and June 13, 2022."[5]

34. On June 24, 2022, LHP determined that Plaintiff's and Class Members' Private Information was present and potentially stolen by the unauthorized person at the time of the incident.[6]

---

[2] Office of the Vermont Attorney General, *https://ago.vermont.gov/blog/2022/08/11/lamoille-health-partners-data-breach-notice-to-consumers/* (last accessed August 24, 2022).
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*

35. Defendant admitted that the stolen information may have included Plaintiff's and Class Members' names, addresses, dates of birth, Social Security numbers, health insurance information, and medical treatment information.

36. LHP also admitted that the Data Breach may have resulted in unauthorized access to the Private Information of Class Members' children, including the child's name, address, date of birth, Social Security number, health insurance information, and medical treatment information.[7]

37. LHP still took nearly three weeks to notify state Attorneys Generals and Class Members about the Data Breach.[8]

38. Upon information and belief, the Private Information was not encrypted prior to the data breach.

39. It is likely the Data Breach was targeted at Defendant due to its status as a healthcare entity that collects, creates, and maintains both PII and PHI.

40. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the Private Information of Plaintiff and the Class Members.

41. As LHP acknowledges in its Notice Letters, protection of personal identifiable information is something it takes "very seriously."[9]

42. Plaintiff and the Class Members reasonably relied (directly or indirectly) on this sophisticated health care institution to keep their sensitive Private Information confidential; to

[7] *Id.*
[8] *Id.*
[9] *Id.*

maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their Private Information.

43. LHP had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' Private Information from involuntary disclosure to third parties.

44. LHP admitted in its *Notice Letter to* the Attorney Generals that its systems were subjected to a ransomware attack and that its data may have been accessed by unauthorized persons' access in July 2022.[10] LHP made no indication to either group (AGs or Class) that the exfiltrated PII was retrieved from the cybercriminals who took it, nor how long the data was available to these unauthorized actors, or if LHP paid any monies to recover the data.

45. With its offer of credit and identity monitoring services to victims, LHP is acknowledging that the impacted persons are subject to an imminent threat of identity theft and financial fraud.

46. In response to the Data Breach, LHP admits it hired a "cybersecurity firm" to "investigate the incident," and purports to have "taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures." LHP admits additional security was required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward.

47. Because of the Data Breach, data thieves were able to gain access to and hold hostage Defendant's IT systems and, were able to compromise, access, and acquire the protected Private Information of Plaintiff and Class Members.

48. Defendant has obligations created by HIPAA, contract law, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to

[10] *Id.*

keep their Private Information confidential and to protect it from unauthorized access and disclosure.

49. Plaintiff's and Class Members' unencrypted, unredacted Private Information was compromised due to LHP's negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' Private Information. Criminal hackers obtained their Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The risks to Plaintiff and Class Members will remain for their respective lifetimes.

Securing PII and Preventing Breaches

50. LHP could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

51. In its notice letters, LHP acknowledged the sensitive and confidential nature of the Private Information. To be sure, collection, maintaining, and protecting Private Information is vital to virtually all of LHP's business purposes as a health care services provider. LHP acknowledged through its conduct and statements that the misuse or inadvertent disclosure of Private Information can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect Private Information from improper release or disclosure.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

52. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII preceding the date of the breach.

53. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[11] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[12] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[13]

54. 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), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

55. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [14]

---

[11] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[12] *Id*.
[13] *Id*.
[14] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

56. 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.[15]

57. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[16]

58. A ransomware attack is a type of cyberattack that is frequently used to target healthcare providers due to the sensitive patient data they maintain.[17] In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[18] Ransomware attacks are particularly harmful for patients and healthcare providers alike as they cause operational disruptions that result in lengthier patient stays, delayed procedures or test results, increased complications from surgery, and even increased mortality rates.[19] In 2021, 44% of healthcare providers who

[15] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360. arn-of-targeted-ransomware (last visited July 2, 2021).
[16] *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.
[17] *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/
[18] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ransomware-faqs
[19] *Ponemon study finds link between ransomware, increased mortality rate*, available at https://www.healthcareitnews.com/news/ponemon-study-finds-link-between-ransomware-increased-mortality-rate

experienced a ransomware attack saw their operations disrupted for up to a week and 25% experienced disrupted services for up to a month.[20]

59. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[21] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

60. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[22] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[23] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[24] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[25]

---

[20] *The State of Ransomware in Healthcare 2022*, available at https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf

[21] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

[22] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

[23] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

[24] *Id.*

[25] *Id.*

61. In light of the above, 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

62. 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.

63. 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.[26] 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.[27]

64. 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

[26] 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).
[27] *Id*.

on the network; and verify that third-party service providers have implemented reasonable security measures.

65. 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.

66. 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.").

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

68. 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.

69. 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

70. 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.

71. Several best practices have been identified that at 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.

72. 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; and training staff regarding critical points.

73. 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.

74. 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 Standards of Care and Evidences Its Insufficient Data Security

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

76. Covered entities (including LHP) must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

77. 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).

78. A Data Breach such as the one Defendant experienced is also 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

79. Data breaches are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[28]

80. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate LHP failed to comply with safeguards and standards of care mandated by HIPAA regulations.

Defendant's Negligent Acts and Breach

81. Defendant breached its obligations to Plaintiff and Class Members and/or 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;

b. Failing to adequately protect patients' Private Information;

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

[28] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf at 4.

d. Failing to train its employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Defendant's networks, and to maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. 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);

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

h. 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);

i. 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);

j. 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);

k. 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);

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

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

n. 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);

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

p. Failing to adhere to industry standards for cybersecurity.

82. As the result of antivirus and malware protection software in dire need of security updating, inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and other failures to maintain its networks in configuration that would protect against cyberattacks like the ransomware intrusion here, Defendant negligently

and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access, and hold hostage, LHP's IT systems, which contained unsecured and unencrypted Private Information.

83. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and Class Members also lost the benefit of the bargain they made with Defendant.

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

84. Data breaches at healthcare providers like Defendant are especially problematic because the breaches can negatively impact the overall daily lives of individuals affected by the attack.

85. For instance, loss of access to patient histories, charts, images, and other information forces providers to limit or cancel patient treatment because of the disruption of service.

86. This leads to a deterioration in the quality of overall care patients receive at facilities affected by data breaches.

87. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[29]

[29] *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 visited Jan. 25, 2022).

88. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[30]

89. Similarly, data breach incidents cause patients issues with receiving care that rise above the level of mere inconvenience. The issues that patients encounter as a result of such incidents include, but are not limited to:

a. rescheduling their medical treatment;

b. finding alternative medical care and treatment;

c. delaying or foregoing medical care and treatment;

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

e. inability to access their medical records.[31]

90. 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."[32]

[30] *See* Sung J. Choi et al., Cyberattack 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 (last visited Jan. 25, 2022).

[31] *See, e.g.*, Lisa Vaas, Cyberattacks Paralyze, and Sometimes Crush, Hospitals, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals// (last visited Jan. 25, 2022); Jessica David, Data Breaches Will Cost Healthcare $4B in 2019. Threats Outpace Tech, Health IT Security (Nov. 5, 2019), https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech - :~:text=November 05, 2019 - Healthcare data,per each breach patient record (last visited Jan. 25, 2022).

[32] *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" (GOA, 2007). Available at https://www.gao.gov/new.items/d07737.pdf. (last visited Jan. 25, 2022).

91. 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 market to identity thieves who desire to extort and harass victims, taking 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.

92. One type of social engineering attack is called a SIM swap. SIM swap attacks are on the rise with the FBI reporting that in 2021, it received 1,611 reports of SIM swap attacks amounting to $68 million in losses to the victims. By contrast, between 2018 and 2020, the FBI received 320 reports of Sim Swaps totaling $12 million in losses to victims.[33] In a SIM swap attack the attacker uses personally identifiable information to impersonate the victim and fool a phone carrier into porting the victim's number to the attacker's phone.[34][35] Once this is

[33] *'SIM swap' scams netted $68 million in 2021: FBI*, available at https://abcnews.go.com/Politics/sim-swap-scams-netted-68-million-2021-fbi/story?id=82900169
[34] *SIM Swapping*, available at https://www.verizon.com/about/account-security/sim-swapping
[35] *SIM Swapping: How the Latest Cellphone Hacking Scam Works, And How to Protect Yourself*, available at https://www.nbcnewyork.com/investigations/sim-swapping-how-the-latest-cellphone-hacking-scam-works-and-how-to-protect-yourself/3686051/

accomplished, calls and texts intended for the victim are instead received by the attacker. The attacker will then use the "forgot password" or two step verification feature on the victim's email accounts, financial accounts, and online shopping accounts to intercept the secret code that the account platform sends to the victim to verify their identity. [36] With this secret code in hand, the attacker can reset the password, lock the victim out of the accounts, and make fraudulent purchases, transfer funds, or impersonate the victim to solicit funds from relatives or associates.

93. In light of the above, 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 (an extended fraud alert that lasts for seven 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.[37]

94. 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.

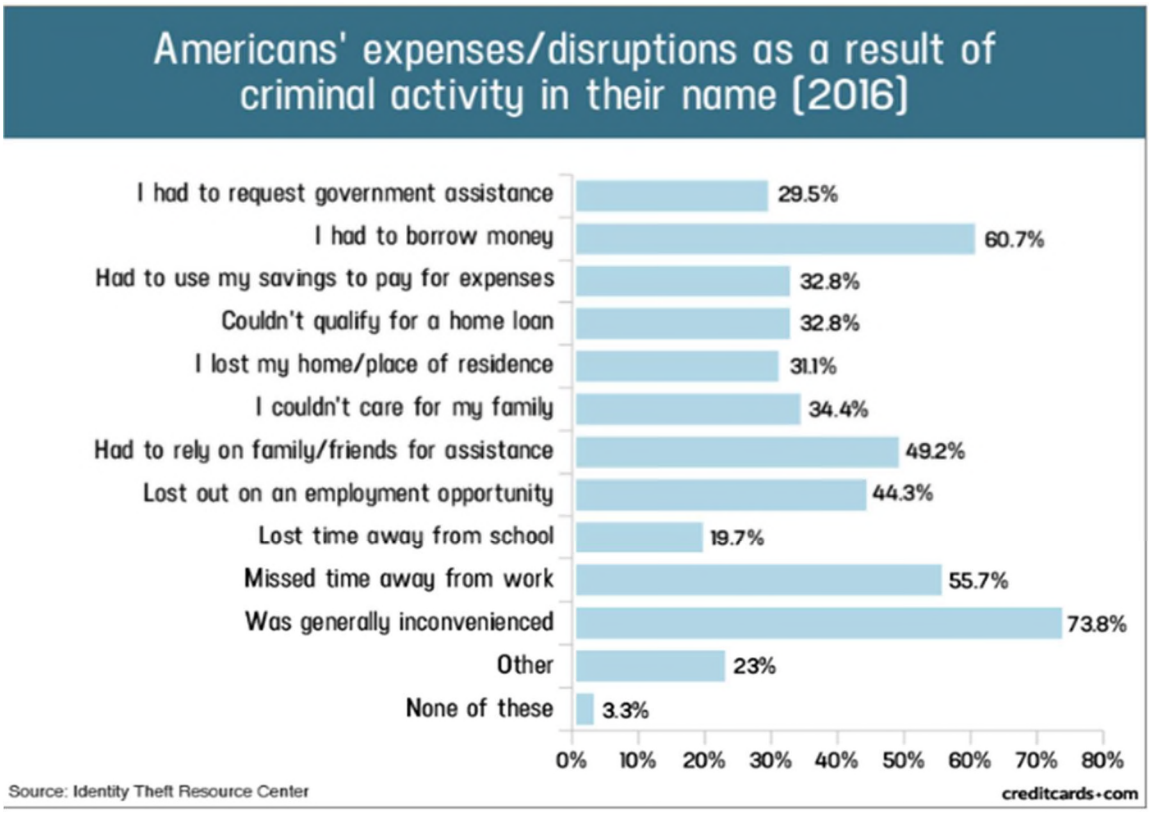
95. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may

[36] *What is SIM swapping? SIM swap fraud explained and how to help protect yourself*, available at https://us.norton.com/internetsecurity-mobile-sim-swap-fraud.html#

[37] *See* IdentityTheft.gov, Federal Trade Commission, https://www.identitytheft.gov/Steps

even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

96. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[38]



97. Moreover, theft of Private Information results in the loss of a valuable property right.[39]

98. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this

[38] *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 visited Jan. 25, 2022).

[39] *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).

obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

99. 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."[40]

100. 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.

101. 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.

102. 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.

[40] *See* Federal Trade Commission, What to Know About Medical Identity Theft, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft identity-theft (last visited Jan. 25, 2022).

103. 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.

104. 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.

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

106. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[41] 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.

107. 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.[42] 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.[43] 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

[41] *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/ (last visited Jan. 25, 2022).
[42] 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 Jan. 25, 2022).
[43] *Id*. at 4.

individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

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

109. 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."

110. 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."

111. Medical information is especially valuable to identity thieves.

112. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[44] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[45]

113. 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.

[44] *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 visited Jan. 25, 2022).
[45] *See* Vaas, Cyberattacks, *supra*, n. 28.

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

115. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach. Defendant has merely offered Plaintiff and Class Members fraud and identity monitoring services for up to twelve (12) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach. Signing up for this service requires Plaintiff and Class Members to forfeit time that could otherwise be spent making money or enjoying life. Moreover, following the expiration of the 12-month subscription, Plaintiff and Class Members will be required to pay for credit monitoring services out of their own pocket.

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

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

118. 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.

119. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

120. Plaintiff and Class Members suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of their Private Information, a form of property that LHP obtained from Plaintiff and Class Members; (b) violation of their privacy rights; (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

121. Plaintiff and Class Members were also injured by and suffered benefit-of-the-bargain damages from this Data Breach. 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 LHP's computer system and network and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

122. Plaintiff and Class Members have suffered or will suffer 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:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

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

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

123. 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 Private Information is not accessible online and that access to such data is password protected.

Plaintiff Marshall's Experience

124. Ms. Patricia Marshall, a citizen and resident of Saint Albans, Vermont received Notice of Data Security Incident Letter dated August 10, 2022 by US. Mail.

125. Plaintiff Marshall received medical care and treatment at LHP in the past. Upon information and belief, during the course of the visits, she was presented with standard medical forms to complete prior to her service that requested her PII and PHI, including HIPAA and privacy disclosure forms.

126. As part of her care and treatment, and as a requirement to receive Defendant's services, Plaintiff Marshall entrusted her PII, PHI, and other confidential information such as name, address, Social Security number, medical and treatment information, and health insurance

information to LHP with the reasonable expectation and understanding that LHP would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff would not have used LHP's services had she known that LHP would not take reasonable steps to safeguard her sensitive PII and PHI.

127. Plaintiff also provided her credit card and banking information for payment of prescription and copays directly to LHP or to its billing vendors.

128. As a result of the Data Breach, Plaintiff Marshall made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

129. Plaintiff experienced actual identify theft and fraud in the form that her Amazon account was accessed by an unauthorized party, forcing Amazon to reverse any modifications made by this unauthorized party, cancelling any pending orders, refunding purchases to Plaintiff's payment instrument, and disabling the two-step verification on Plaintiff's account. Amazon further noted that her account would be deactivated if she did not respond within 24 hours.

130. Plaintiff also received telephone calls from unknown parties stating that unauthorized parties had purchased computers on her Amazon account.

131. Plaintiff Marshall has spent a significant number of hours reviewing her bank accounts, contacting her bank, and contacting other businesses, and will continue to spend valuable time Plaintiff Marshall otherwise would have spent on other activities, including but not limited to work and/or recreation.

132. Plaintiff Marshall is very careful about sharing her own personal identifying information and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

133. Plaintiff destroys any documents she receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

134. Plaintiff Marshall suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII and PHI, a form of property that LHP obtained from Plaintiff Marshall; (b) violation of her privacy rights;(c) the likely theft of her PII and PHI; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

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

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

137. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in LHP's possession, is protected and safeguarded from future breaches.

Class Allegations

138. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated.

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

> All persons residing in the United States whose Private Information was compromised in the data breach announced by LHP in August 2022. (the "Nationwide Class").

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

141. Plaintiff reserves the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

142. Numerosity. The Members of the Class 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 Class consists of approximately 59,000 individuals whose sensitive data was compromised in Data Breach.

143. Commonality. There are questions of law and fact common to the Class, 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;

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

h. Whether Defendant should have discovered the Data Breach sooner;

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

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breach implied contracts with Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

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

144. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

145. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

146. 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.

147. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual

Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

148. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

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

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

151. Adequate notice can be given to Class Members directly using information maintained in LHP's records.

152. Unless a Class-wide injunction is issued, LHP may continue in its failure to properly secure the PII of Class Members, LHP may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and LHP may continue to act unlawfully as set forth in this Complaint.

153. Further, LHP has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive relief with regard to the Class Members as a whole is appropriate.

Causes f Action

COUNT I
Negligence
(On Behalf of Plaintiff and All Class Members)

154. Plaintiff restates and realleges all of the foregoing paragraphs as if fully set forth herein.

155. Defendant LHP required Plaintiff and Class Members to submit non-public personal information in order to obtain healthcare and/or healthcare related services.

156. By collecting and storing this data in LHP's 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 their 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 it

could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

157. 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.

158. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant LHP and its 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 or data breach.

159. 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)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

160. 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.

161. 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.

162. Defendant breached its duties, and thus were 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 email 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 secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

163. 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 cyberattacks and data breaches in the healthcare industry.

164. 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.

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

166. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

167. 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
Unjust Enrichment
(On Behalf of Plaintiff and All Class Members)

168. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

169. Plaintiff brings this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of contract count below.

170. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

171. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

172. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing 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 have their Private Information protected with adequate data security.

173. 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.

174. 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.

175. 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.

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

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

178. 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.

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

180. 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.

181. 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.

182. 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.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and All Class Members)

183. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

184. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

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

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

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

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

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

190. 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 their 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.

191. As a direct and proximate result of Defendant's breach 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
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

192. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

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

194. Defendant solicited, offered, and invited 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.

195. 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.

196. Plaintiff and Class Members paid money to Defendant or provided labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

197. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

198. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

199. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

200. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

201. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

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

203. Plaintiff and 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.

Prayer for Relief

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to

identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated: Burlington, Vermont
September 1, 2022

for: Matthew B. Byrne, Esq.
Gravel & Shea PC
76 St. Paul Street, 7th Floor, P.O. Box 369
Burlington, VT 05402-0369
(802) 658-0220
mbyrne@gravelshea.com

Gary M. Klinger (*pro hac vice* forthcoming)
Milberg Coleman Bryson Phillips
Grossman, PLLC
227 Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

David K. Lietz (*pro hac vice* forthcoming)
Milberg Coleman Bryson Phillips
Grossman, Pllc
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
Email: dlietz@milberg.com

Terence R. Coates*
Justin C. Walker*
Markovits, Stock & Demarco, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com
**pro hac vice* forthcoming

Attorneys for Plaintiff and the Proposed Class