COMMONWEALTH OF MASSACHUSETTS

BRISTOL, ss

SUPERIOR COURT
CIVIL ACTION NO. 2473CV00710

ROBERT WOODWARD and TIMOTHY KING, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

NORTH COTTAGE PROGRAM, INC.,

Defendant.

AMENDED COMPLAINT—CLASS ACTION

PLAINTIFFS' AMENDED CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiffs Robert Woodward and Timothy King ("Plaintiffs"), individually and on behalf of all others similarly situated, sue Defendant North Cottage Program, Inc. ("Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

I. INTRODUCTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant (the "Data Breach"), which held in its possession certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information") of Plaintiffs and other current and former clients of Defendant, the putative class members ("Class"). This Data Breach occurred on or around May 16, 2024.

2. The Private Information compromised in the Data Breach included certain personal or protected health information of Defendant North Cottage Program, Inc.'s, current and former

clients, including Plaintiffs. This Private Information included but is not limited to "name, address, Social Security number, date of birth, treatment plan, medication information, health insurance information, and provider notes."[1]

3. The Private Information was copied by cyber-criminals who perpetrated the attack and remains in the hands of those cyber-criminals. According to Defendant's report to the U.S. Department of Health and Human Services Office of Civil Rights, 8,190 individuals were affected.[2]

4. The Data Breach resulted from Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which they were entrusted for treatment.

5. Plaintiffs bring 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 Plaintiffs and other Class Members that their information was subjected to unauthorized access by an unknown third party and precisely what type of information was accessed.

6. 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. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' 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.

---

[1] Defendant North Cottage Program, Inc., *Notice of Data Security Incident*, *available at* http://www.northcottage.com/page31.html (*last accessed* September 27, 2024).
[2] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (*last accessed* September 27, 2024).

7. Defendant, through its employees, disregarded the rights of Plaintiffs and Class Members (defined below) by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions. Defendant also failed to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' Private Information and failed to take standard and reasonably available steps to prevent the Data Breach.

8. In addition, Defendant's employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant's employees (presumably in the IT department) properly monitored its property, it would have discovered the intrusion sooner.

9. Plaintiffs' 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.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes. These crimes include opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims 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.

11. Because of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiffs and Class Members may also 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.

13. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiffs seek 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.

15. Accordingly, Plaintiffs sue Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract, and (iv) breach of fiduciary duty.

II. PARTIES

16. Plaintiff Robert Woodward is and at all times mentioned herein was an individual citizen of Massachusetts, residing in the city of Norton.

17. Plaintiff Timothy King is and at all times mentioned herein was an individual citizen of Massachusetts, residing in the city of Hanson.

18. Defendant North Cottage Program, Inc., is a Massachusetts-based non-profit corporation that offers healthcare services including inpatient addiction treatment to clients in the

vicinity of Norton. Defendant's principal place of business is 69 East Main Street, Norton, Massachusetts, 02766.

III. JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action pursuant to Mass Gen. Laws ch. 212 § 4 because Plaintiffs seek injunctive relief and damages in excess of $50,000.00.

20. This Court has general personal jurisdiction over Defendant pursuant to Mass Gen. Laws ch. 223A § 2 because Defendant is domiciled and has its principal place of business in the commonwealth of Massachusetts.

21. Venue is proper in this Court because Defendant maintains its principal place of business within Bristol County, Massachusetts, and because a substantial part of the acts or omissions giving rise to this action occurred within this county.

IV. FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

22. Defendant offers healthcare services including inpatient addiction treatment to clients in and around Norton, Massachusetts.

23. In the ordinary course of receiving health care services from Defendant, each client must provide (and Plaintiffs did provide) Defendant with sensitive, personal, and private information, such as his or her:

- address;
- telephone number;
- date of birth;
- Social Security number;
- Medical history.

24. All of Defendant's employees and staff may share patient information with each other for various purposes, as should be disclosed in a HIPAA compliant privacy notice ("Privacy Policy") that Defendant is required to maintain.

25. Upon information and belief, Defendant's HIPAA Privacy Policy is provided to every patient prior to receiving treatment and upon request.

26. Defendant agreed to and undertook legal duties to maintain the protected health and personal information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws, including the Health Insurance Portability and Accountability Act ("HIPAA").

27. The patient and employee information held by Defendant in its computer system and network included the Private Information of Plaintiffs and Class Members.

THE DATA BREACH

28. A Data Breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

29. The Notice of Data Security Incident posted to Defendant's website describes the Data Breach as follows:

> What Happened NCP experienced a network security incident that involved an unauthorized party gaining access to our network environment on May 16, 2024. Upon detecting the incident, we immediately shut off all access to the network and engaged a specialized third-party forensic incident response firm to assist with securing the network environment and investigating the extent of unauthorized activity. The forensic investigation determined that the unauthorized third party may have acquired certain data as a result of this incident. After conducting a comprehensive review of the data potentially impacted in this incident, which was completed on August 12, 2024, we determined that the unauthorized third party may have acquired certain personal information as a result of this incident. NCP is providing written notice to all impacted individuals. NCP has no reason to believe that any individual's information has been misused as a result of this event. As of this writing, NCP has not received any reports of misuse of information and/or related identity theft since the date the incident was discovered (May 16, 2024 to present).
>
> What Information Was Involved Again, we found no evidence that patient information has been specifically misused. However, the following information was potentially exposed to an unauthorized third party: first name, last name, address, Social Security number, date of birth, treatment

plan, medication information, health insurance information, and provider notes.

30. The U.S. Department of Health and Human Services requires, "[i]f a breach of unsecured protected health information affects *500 or more individuals*, a covered entity must notify the Secretary of the breach without unreasonable delay and in *no case later than 60 calendar days* from the discovery of the breach."[3] Further, if "the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate," and later provide an addendum or correction to HSS.[4]

31. Defendant cannot claim it was unaware of the HHS notification requirements as it complied (at least in part) with those requirements.

32. Defendant's notice letter were dated August 30, 2024—around three months after the data breach occurred.

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

34. Plaintiffs 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.

35. 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.

[3] U.S. Department of Health and Human Services, *Submitting Notice of a Breach to the Secretary* (Feb. 27, 2023) https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last viewed September 27, 2024) (emphasis added).
[4] *Id.*

36. In 2023, a record 3,205 data breaches occurred, resulting in around 353,027,892 individuals' information being compromised, a 78% increase from 2022.[5] Of the 2023 recorded data breaches, 809 of them, or 25%, were in the medical or healthcare industry.[6] The 809 reported breaches reported in 2023 exposed nearly 56 million sensitive records, compared to only 343 breaches that exposed just over 28 million sensitive records in 2022.[7]

37. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

38. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[8]

39. 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.

"QILIN" AND THE DARK WEB

40. To make matters worse, the cybercriminals that obtained Plaintiffs' and Class Members' Private Information were the notorious cybercriminal group "Qilin" who claimed responsibility for the data breach on June 4, 2024.[9]

---

[5] *See* Identity Theft Resource Center, *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last visited June 10, 2024).
[6] *Id*.
[7] *Id*. at 11, Fig.3.
[8] Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), *available at* https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited May 21, 2024).
[9] Paul Bischoff, *Massachusetts halfway house client data breached, SSNs and medical info compromised*, COMPARITECH (Sept. 10, 2024) https://www.comparitech.com/news/massachusetts-halfway-house-client-data-breached-ssns-and-medical-info-compromised/.

41. The federal Health Sector Cybersecurity Coordination Center released a "threat profile" on Qilin (aka "Agenda") on June 18, 2024.[10] Therein, the federal agency explained that:

a. "The group likely originates from Russia[.]"[11]

b. "The group has steadily increased its activity over the past year, claiming responsibility for more than 60 ransomware attacks since January 2024."[12]

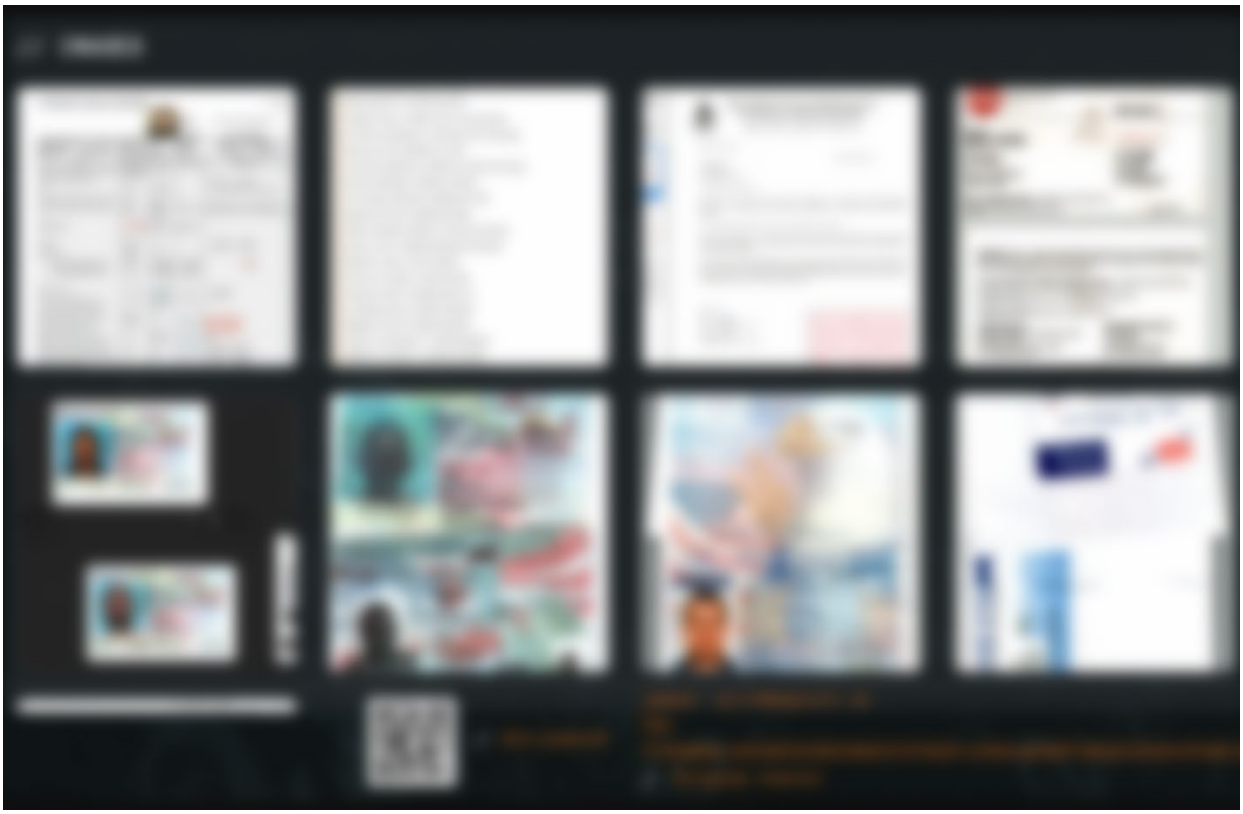
c. "Victims are directed to communicate with the attackers via dark web portals or encrypted messaging services, ensuring the attackers' anonymity and complicating law enforcement efforts to track interactions."[13]

d. "Agenda actors practice double extortion and operate a data leak site (DLS) where victims are posted."[14]

42. Worryingly, Qilin already leaked stolen Private Information on the Dark Web.[15] A screenshot of Qilin's Dark Web leak page shows that Qilin posted medical records (along with photos) and scans of identification documents (including Massachusetts driver licenses and a US passport).[16] Additionally, the Dark Web leak page provided a QR code and password—which, on information and belief, allow other cybercriminals to access the stolen Private Information.[17] A screenshot of the Dark Web leak page is provided below—however, it has been blurred to protect the privacy of the victims.

---

[10] *HC3: Threat Profile*, HHS.GOV (June 18, 2024) https://www.hhs.gov/sites/default/files/qilin-threat-profile-tlpclear.pdf,
[11] *Id*.
[12] *Id*.
[13] *Id*.
[14] *Id*.
[15] Paul Bischoff, *Massachusetts halfway house client data breached, SSNs and medical info compromised*, COMPARITECH (Sept. 10, 2024) https://www.comparitech.com/news/massachusetts-halfway-house-client-data-breached-ssns-and-medical-info-compromised/.
[16] *Qilin*, RANSOMLOOK, https://www.ransomlook.io/group/qilin (last visited Dec. 17, 2024).
[17] *Id*.



43. Despite the broad and public leaking of Private Information by Qilin, Defendant misled Plaintiffs and Class Members about the severity of its Data Breach when it declared in its data breach notices that:

a. "NCP has found no evidence that your information has been misused."[18]

b. "Again, we have no evidence that your information has been misused."[19]

c. "[W]e have no indication at this time of any misuse of your information[.]"[20]

[18] *Notice of Data Incident*, MASS.GOV (Aug. 30, 2024) https://www.mass.gov/doc/2024-1623-north-cottage-program/download.
[19] *Id*.
[20] *Id*.

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

44. The Federal Trade Commission ("FTC") has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

45. 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.[21] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor incoming traffic for activity suggesting 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.[22]

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

47. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and

[21] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), *available at* www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 19, 2024).
[22] *Id*.

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 also clarify the measures businesses must take to meet their data security obligations.

48. 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.").

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

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

51. Defendant was always fully aware of its obligation to protect the PII and PHI of its clients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

52. 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.

53. 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; using strong passwords; creating multi-layer security, including firewalls, antivirus, and anti-

malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data; and limiting which employees can access sensitive data.

54. 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.

55. 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.

56. 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 MASSACHUSETTS REGULATIONS

57. Massachusetts General Laws Ch. 93 § 2 empowers the department of consumer affairs and business regulation to "adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth."

58. 201 C.M.R. § 17.04 requires persons who own or license personal information, including Defendant, to adopt specific procedures for the protection of personal information, such as:

(a) control of user IDs and other identifiers;

(b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
(c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
(d) restricting access to active users and active user accounts only; and
(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.

59. Massachusetts regulations further require persons who own or license personal information to monitor systems for unauthorized access, encrypt personal information that is transmitted over public networks or stored on portable devices, keep software reasonably up to date, and educate employees on the importance of personal information security.

60. Defendant negligently failed to implement one or more of the security precautions required by state regulations, thereby exposing Plaintiffs' and Class Members' personal information to data thieves.

DEFENDANT'S CONDUCT VIOLATES HIPAA AND REVEALS 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. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

63. 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 PHI 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).

64. A Data Breach 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. *See* 45 C.F.R. 164.402 (Defining "Breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information.").

65. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to meet standards mandated by HIPAA regulations.

V. DEFENDANT'S BREACH

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

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

b. Failing to adequately protect clients' Private Information;

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

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

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

f. 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);

g. 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);

h. 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);

i. 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);

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

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

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

m. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they 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 C.F.R. § 164.304, definition of "encryption").

67. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing ransomware or other malignant code, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

68. Plaintiffs and Class Members now face an increased risk of fraud and identity theft.

DATA BREACHES PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

69. Data Breaches such as the one experienced by Defendant's clients are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

70. 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."[23]

71. 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 (possibly 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.[24]

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

73. 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 even give

[23] U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf (last visited May 21, 2024) ("GAO Report").
[24] Federal Trade Commission, *What To Do Right Away* (2024), *available at* https://www.identitytheft.gov/Steps (last visited August 19, 2024).

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

74. Theft of Private Information is gravely serious. PII/PHI is a valuable property right.[25] Its value is axiomatic, considering the value of Big Data in corporate America and 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.

75. Theft of PHI is also 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."[26] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

76. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which studied 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

[25] *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).

[26] *See* Federal Trade Commission, *Medical Identity Theft*, *available at* http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited May 21, 2024).

> 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.

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

78. There is a strong probability that all the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

79. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[27] 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.

80. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for more credit lines.[28] 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.[29] Each of these fraudulent

[27] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), *available at* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited May 21, 2024).
[28] Social Security Administration, *Identity Theft and Your Social Security Number* (2018), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 21, 2024).
[29] *Id* at 4.

activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

81. It is also hard to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[30]

82. Healthcare data, because of its sensitivity, demands a much higher price on the black market. The National Association of Healthcare Access Management reports, "[p]ersonal medical data is said to be more than ten times as valuable as credit card information."[31]

83. Medical information is especially valuable to identity thieves. 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. That pales in comparison with the asking price for medical data, which was selling for $300 and up.[32]

84. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore

[30] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (February 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited May 21, 2024).
[31] Laurie Zabel, *The Value of Personal Medical Information: Protecting Against Data Breaches*, NAHAM Connections, *available at* https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information (last visited August 30, 2024).
[32] Paul Ducklin, *FBI "ransomware warning" for healthcare is a warning for everyone!*, Sophos (Oct. 29, 2020) *available at* https://news.sophos.com/en-us/2020/10/29/fbi-ransomware-warning-for-healthcare-is-a-warning-for-everyone/ (last visited March 10, 2022).

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

VI. PLAINTIFF ROBERT WOODWARD'S EXPERIENCE

85. Plaintiff Robert Woodward is and at all times mentioned herein was an individual citizen residing in the State of Massachusetts, in the city of Norton.

86. Plaintiff provided Defendant with his sensitive Private Information as a condition of receiving treatment from Defendant. Plaintiff received notice of the Data Breach around August 30, 2024, informing him that his sensitive information was part of Defendant's Data Breach, including his "name, address, Social Security number, date of birth, treatment plan, medication information, health insurance information, and provider notes"—which includes PHI.

87. Plaintiff reasonably expected and understood that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard his Private Information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to the same.

88. Plaintiff is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff also stores any documents containing his sensitive information in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

89. Because of the Data Breach and at the recommendation of Defendant and its Notice, Plaintiff made reasonable efforts to mitigate the effect of the Data Breach, including, but not limited to, researching the Data Breach, reviewing financial statements, and monitoring his credit information.

90. Plaintiff has spent much time responding to the dangers from the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to work and recreation.

91. Plaintiff is especially alarmed by the amount of stolen or accessed PII and PHI listed in Defendant's notice letter. Despite Defendant providing that list, Plaintiff cannot be sure whether more of his PII or PHI was exfiltrated.

92. Plaintiff has spent several hours of time reviewing his Private Information and monitoring his credit and intends to do so on an ongoing basis. He has also experienced a serious uptick in spam calls since the Data Breach incident.

93. Plaintiff knows that cybercriminals often sell Private Information, and that his PII or PHI could be abused months or even years after a data breach.

94. Had Plaintiff been aware that Defendant's computer systems were not secure, he would not have entrusted Defendant with his personal data.

VII. PLAINTIFF TIMOTHY KING'S EXPERIENCE

95. Plaintiff Timothy King is and at all times mentioned herein was an individual citizen residing in the State of Massachusetts, in the city of Hanson.

96. Plaintiff provided Defendant with his sensitive Private Information as a condition of receiving treatment from Defendant. Plaintiff received notice of the Data Breach on or around September 19, 2024, information him that his Private Information was part of Defendant's Data Breach, including his "name, address, Social Security number, date of birth, treatment plan, medication information, health insurance information, and provider notes."

97. Plaintiff reasonably expected and understood that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard his Private

Information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to the same.

98. Plaintiff is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff also stores any documents containing his sensitive information in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

99. Because of the Data Breach and at the recommendation of Defendant and its Notice, Plaintiff made reasonable efforts to mitigate the effect of the Data Breach, including, but not limited to, researching the Data Breach, reviewing financial statements, and monitoring his credit information.

100. Plaintiff has spent much time responding to the dangers from the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to work and recreation.

101. Plaintiff has spent several hours freezing his credit and enrolling in credit monitoring.

102. Plaintiff is especially alarmed by the amount of stolen or accessed PII and PHI listed in Defendant's notice letter. Despite Defendant providing that list, Plaintiff cannot be sure whether more of his PII or PHI was exfiltrated.

103. Plaintiff has received a dramatic uptick in spam calls since Defendant's Data Breach.

104. Plaintiff knows that cybercriminals often sell Private Information, and that his PII or PHI could be abused months or even years after a data breach.

105. Had Plaintiff been aware that Defendant's computer systems were not secure, he would not have entrusted Defendant with his personal data.

VIII. PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

106. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered 24 months of inadequate identity monitoring services, despite Plaintiffs and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

107. The 24 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

108. Furthermore, Defendant's credit monitoring advice to Plaintiffs and Class Members places the burden on Plaintiffs and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach.

109. Plaintiffs and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

110. Plaintiffs' Private Information was compromised and exfiltrated by cyber criminals as a direct and proximate result of the Data Breach.

111. Plaintiffs were damaged in that their Private Information is in the hands of cyber criminals.

112. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

113. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

114. Plaintiffs 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.

115. Plaintiffs 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 more effectively target such schemes to Plaintiffs and Class Members.

116. Plaintiffs 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.

117. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber criminals in the Data Breach. Many courts have recognized the propriety of loss of value damages in related cases.

118. Plaintiffs 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. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

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

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

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

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

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

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

j. Paying late fees and declined payment fees imposed because of failed automatic payments that were tied to compromised cards that had to be cancelled; and

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

119. Moreover, Plaintiffs 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 implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password protected.

120. Further, because of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

121. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

IX. CLASS ACTION ALLEGATIONS

122. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

123. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> **All persons whose Private Information was compromised because of the May, 2024 Data Breach (the "Class").**

124. Excluded from the Class are Defendant's officers and directors, and 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.

125. Plaintiffs reserve the right to amend or modify the class definitions with greater specificity or division after having an opportunity to conduct discovery. The proposed Class meets the criteria for certification under Rule 23 of the Massachusetts Rules of Civil Procedure.

126. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiffs now, but Defendant has provided notice to the Health and Human Services Office of Civil Rights that 8,190 individuals were affected.

127. 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 Plaintiffs' 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 adhered to 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 Plaintiffs and Class Members suffered legally cognizable damages from Defendant's misconduct;

i. Whether Defendant's conduct was negligent;

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

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

l. Whether Defendant failed to provide notice of the Data Breach promptly; and

m. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

128. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, among other things, all Class Members were injured through the common misconduct of Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and no defenses are unique to Plaintiffs. Plaintiffs' claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

129. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

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

131. 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.

132. 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.

133. Further, issues that will arise in this case are appropriate for class certification because such issues are common to the Class, the resolution of which would advance the matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect its data systems were reasonable considering best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

134. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

X. CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiffs and All Class Members)

135. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

136. Defendant required Plaintiffs and Class Members to submit non-public personal information to obtain healthcare services.

137. By collecting and storing this data in Defendant'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 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 it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

138. Defendant owed a duty of care to Plaintiffs 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.

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

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

141. 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.

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

143. 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 its networks and systems;

c. Failing to periodically ensure that its 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 timely 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.

144. 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.

145. 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.

146. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

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

148. Plaintiffs 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) provide adequate credit monitoring to all Class Members.

SECOND COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and All Class Members)

149. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

150. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

151. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

152. In entering such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and adhered to industry standards.

153. Plaintiffs and Class Members paid money to Defendant or had money paid on their behalf with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

154. Plaintiffs 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.

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

156. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

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

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

159. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

160. Plaintiffs 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.

THIRD COUNT
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and All Class Members)

161. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

162. Under the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

163. Under HIPAA, 42 U.S.C. § 1302d, *et seq*., Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

164. Under HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, 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." See definition of encryption at 45 C.F.R. § 164.304.

165. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

166. Under 201 C.M.R. § 17.03, *et seq.*, Defendant had a duty to "maintain a comprehensive information security program" that includes minimum protocols for computer security.

167. Defendant breached its duties under applicable Massachusetts regulations by failing to maintain computer security appropriate to the sensitive private information Defendant collected and stored.

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

169. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

170. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that by failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

171. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FOURTH COUNT
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and All Class Members)

172. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

173. Defendant became guardian of Plaintiffs' and Class Members' Private Information, creating a special relationship between Defendant and Plaintiffs and Class Members.

174. As such, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs 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.

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

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

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

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

179. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the compromise, publication, and/or theft of their Private Information;

c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;

e. 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;

f. future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the rest of the lives of Plaintiffs and Class Members; and

g. the diminished value of Defendant's services they received.

180. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH COUNT
INVASION OF PRIVACY
(On Behalf of Plaintiffs and All Class Members)

181. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

182. Massachusetts law recognizes the personal right to privacy and the right to enforce one's right to privacy. *See* M.G.L., c. 214, § 1B. 229.

183. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

184. Defendant owed a duty to its current and former clients, including Plaintiffs and the Class, to keep this information confidential.

185. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class Members' Private Information is highly offensive to a reasonable person.

186. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

187. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

188. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

189. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

190. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

191. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiffs and the Class were stolen by a third party and is now available

for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed supra).

192. And, on information and belief, Plaintiffs' Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

193. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

194. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiffs and the Class.

195. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class Members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

SIXTH COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and All Class Members)

196. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

197. This claim is pleaded in the alternative to the breach of implied contract claim.

198. Plaintiffs and Class Members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their Private Information to provide services, and (2) accepting payment.

199. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class Members.

200. Plaintiffs and Class Members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

201. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information.

202. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

203. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class Members' (1) Private Information and (2) payment because Defendant failed to adequately protect their Private Information.

204. Plaintiffs and Class Members have no adequate remedy at law.

205. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

SEVENTH COUNT
VIOLATIONS OF THE MASSACHUSETTS CONSUMER PROTECTION ACT
MASS. GEN. LAWS. ANN. CH. 93A, §§ 1, *ET SEQ*.
(On Behalf of Plaintiffs and All Class Members)

206. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

207. Defendant, Plaintiffs and Class Members are "persons" as meant by Mass. Gen. Laws. Ann. Ch. 93A, § 1(a).

208. Defendant engages in "trade or commerce" under Mass. Gen. Laws. Ann. Ch. 93A, § 1(b).

209. Defendant advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

210. Defendants engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including by:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

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

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Private Information; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

211. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their Private Information.

212. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its omissions.

213. Had Defendant disclosed to Plaintiffs and Class Members (or their third-party agents) that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

214. Defendant accepted the Private Information that Plaintiffs and Class Members entrusted to it while keeping the inadequate state of its security controls secret from the public.

215. Accordingly, Plaintiffs and Class Members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

216. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiffs' and Class Members' rights.

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

218. On information and belief, Plaintiffs' Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

219. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law.

XI. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above seeks the following relief:

a. For an Order certifying this action as a class action, defining the Class as requested herein, appointing Plaintiffs and their counsel to represent the Class, and finding that Plaintiffs is a proper representative of the Class requested herein;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For an order directing Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

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

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

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

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

i. Any other relief that this court may deem just and proper.

XII. JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: January 14, 2025

Respectfully submitted,

/s/ John P. Kristensen

John P. Kristensen, BBO # 712688
KRISTENSEN LAW GROUP
53 State Street, Suite 500
Boston, MA 02109
Telephone: (617) 913-0363
john@kristensen.law

Leigh S. Montgomery*
Texas Bar No. 24052214
EKSM, LLP
1105 Milford Street
Houston, Texas 77006
Telephone: (888) 350-3931
lmontgomery@eksm.com

Michael S. Appel (BBO# 543898)
KETTERER, BROWNE & ASSOCIATES, LLC
336 S. Main Street
Bel Air, Maryland 21014
Telephone: (617) 359-4981
michael@KBAattorneys.com

Cassandra P. Miller*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Telephone: 872.263.1100
cmiller@straussborrelli.com

ATTORNEYS FOR PLAINTIFF
(* denotes *pro hac vice* forthcoming)

CERTIFICATE OF SERVICE

I, John P. Kristensen, counsel for Plaintiff Robert Woodward, and hereby certify that on this 14th day of January, 2025, I served the foregoing, ***PLAINTIFFS' AMENDED CLASS ACTION COMPLAINT AND JURY DEMAND***, via Electronic Mail to the following counsel:

Leigh S. Montgomery*
Texas Bar No. 24052214
EKSM, LLP
1105 Milford Street
Houston, Texas 77006
Telephone: (888) 350-3931
lmontgomery@eksm.com

Co-Counsel for Plaintiffs

Cassandra P. Miller*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Telephone: 872.263.1100
cmiller@straussborrelli.com

Co-Counsel for Plaintiffs

Michael S. Appel (BBO# 543898)
KETTERER, BROWNE & ASSOCIATES, LLC
336 S. Main Street
Bel Air, Maryland 21014
Telephone: (617) 359-4981
michael@KBAattorneys.com

Co-Counsel for Plaintiffs

Thomas C. Blatchley (BBO#706212)
GORDON & REES SCULLY MANSUKHANI, LLP
28 State Street, Suite 1050
Boston, MA 02109
Phone: 860-278-7448
Fax: 860-560-0185
tblatchley@grsm.com

Counsel for Defendant North Cottage Program, Inc.