

James C. Shah  
Natalie Finkelman Bennett  
**MILLER SHAH LLP**  
2 Hudson Place, Suite 100  
Hoboken, NJ 07030  
Tel: (866) 540-5505  
Fax: (866) 300-7367  
[jcshah@millershah.com](mailto:jcshah@millershah.com)  
[nfinkelman@millershah.com](mailto:nfinkelman@millershah.com)

Amber L. Schubert (*pro hac vice* to be filed)  
**SCHUBERT JONCKHEER & KOLBE LLP**  
2001 Union St., Suite 200  
San Francisco, CA 94123  
Tel: (415) 788-4220  
Fax: (415) 788-0161  
[aschubert@sjk.law](mailto:aschubert@sjk.law)

*Counsel for Plaintiff*

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEW JERSEY  
CAMDEN DIVISION**

LACY MATCZAK, Individually and on Behalf  
of a Class of All Others Similarly Situated,

Plaintiff,

v.

COMMUNITY HEALTH CARE, INC. d/b/a  
COMPLETECARE HEALTH NETWORK,

Defendant.

Case No.

**CLASS ACTION COMPLAINT**

Jury Trial Demanded

Upon personal knowledge as to her own acts, and based upon her investigation, the investigation of counsel, and information and belief as to all other matters, Plaintiff Lacy Matczak, on behalf of herself and all others similarly situated, alleges against Defendant

Community Health Care, Inc. d/b/a CompleteCare Health Network (“CCHN” or “Defendant”) as follows:

### **SUMMARY OF THE ACTION**

1. This action arises out of a targeted cyberattack and data breach caused by Defendant’s failure to secure and safeguard Plaintiff’s and other individuals’ personally identifying information (“PII”) and personal health information (“PHI”), including their names, addresses, Social Security numbers, and medical records (the “Data Breach”).

2. Defendant CCHN is a New Jersey-based healthcare services provider and operates more than a dozen facilities. Defendant claims to employ at least 258 doctors and staff and to serve over 60,000 patients annually.<sup>1</sup>

3. As part of conducting its affairs, Defendant CCHN acquired, collected, and stored consumers’ personal data, including PII and PHI (collectively, “Private Information”).

4. By at least October 12, 2023, an unauthorized party gained access to CCHN’s computer systems. During that time, the hackers accessed highly confidential Private Information of CCHN patients including data on Plaintiff.

5. The unauthorized party obtained files from CCHN containing the Private Information of at least 313,973 people.

6. According to Defendant CCHN, the Private Information compromised in the Data Breach included: patient names, addresses, phone numbers, Social Security numbers, medical information, and other sensitive information provided to CCHN.<sup>2</sup>

---

<sup>1</sup> <https://completecarenj.org> (Last accessed February 5, 2024)

<sup>2</sup> See *Data Breach Letter* (Exhibit 1)

7. On or about December 15, 2023, Defendant sent out a data breach notification advising patients, including Plaintiff, that CompleteCare had been targeted by a sophisticated ransomware attack, which was detected and purportedly stopped on or around October 12, 2023.

8. Plaintiff received services from CCHN. Plaintiff learned of the Data Breach when he received a notice from Defendant dated December 15, 2023, more than two months after the Data Breach was detected, stating that Plaintiff's Private Information was exposed in the Data Breach. This was not received until on or about December 27, 2023.

9. The Data Breach was a direct result of the failure by Defendant to implement reasonable cybersecurity procedures to protect the Private Information of Plaintiff and the Class, as defined below.

10. Plaintiff, individually and on behalf of all others similarly situated, alleges claims against Defendant for (i) negligence; (ii) breach of implied contract; and (iii) unjust enrichment.

11. Plaintiff, individually and on behalf of all others similarly situated, asks the Court to compel Defendant to adopt reasonable information security practices to secure the sensitive Private Information that they collect and store in their databases and to grant such other relief as the Court deems just and proper.

## **PARTIES**

### **A. Plaintiff**

12. Plaintiff Lacy Matczak is a resident and citizen of Delaware. She obtained services from CCHN and subsequently received a notice from Defendant, dated December 15, 2023, that her Private Information had been compromised.

**B. Defendant**

18. Defendant Community Health Care, Inc. d/b/a CompleteCare Health Network (CCHN). Defendant CCHN is a New Jersey-based healthcare services provider and operates more than a dozen facilities. Defendant claims to employ at least 258 doctors and staff and to serve over 60,000 patients annually.

**JURISDICTION AND VENUE**

19. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because Plaintiff and at least one member of the putative Class, as defined below, is a citizen of a state other than that of Defendant, there are more than 100 putative Class Members, and the aggregate amount in controversy exceeds \$5,000,000, exclusive of interest and costs.

20. This Court has general personal jurisdiction over Defendant because it maintains its principal place of business in New Jersey, regularly conduct business in New Jersey, and has sufficient minimum contacts in New Jersey, such as to not offend traditional notions of fair play and substantial justice.

21. Venue in this District is proper under 28 U.S.C. § 1391 because Defendant resides in this District and a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District, including Defendant collecting and storing the Private Information of Plaintiff and the putative Class Members.

## **FACTUAL BACKGROUND**

### **A. Defendant Collected, Stored, and Maintained Huge Amounts of Their Patients' Private Information.**

22. Defendant CCHN is one of the largest federally qualified health centers in New Jersey and operates at least 14 different locations.<sup>3</sup>

23. On information and belief, in the ordinary course of providing healthcare services to their patients, Defendant collected their patients' Private Information, including but not limited to:

- a. Names
- b. Dates of birth
- c. Addresses
- d. Demographic information
- e. Social Security numbers
- f. Taxpayer identification numbers
- g. Medical Record numbers
- h. Medical histories
- i. Treatment information
- j. Diagnosis information
- k. Diagnosis codes
- l. Mental/Physical conditions
- m. Prescription information
- n. Providers' information
- o. Health insurance information
- p. Beneficiaries' information
- q. Billing and claims information
- r. Patient account numbers
- s. Patient identification numbers
- t. Treatment cost information

24. As a condition of receiving treatment, Defendant requires that their patients entrust them with highly sensitive personal information. Additionally, Defendant may receive Private Information from other individuals and organizations that are part of a patient's "circle of

---

<sup>3</sup> <https://completecarenj.org> (last accessed February 5, 2024)

care,” such as referring physicians, other doctors, customers’ health plans, and close family and friends.

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 they were responsible for protecting Plaintiff’s and Class Members’ Private Information from disclosure.

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

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

28. Defendant even acknowledges in their privacy policy that “We are legally required to maintain the privacy of your health information.”<sup>4</sup>

**B. Defendant’s Data Breach Exposed Patients’ Valuable Private Information.**

29. Defendant collected and maintained Plaintiff’s and the Class’s Private Information in their computer systems, servers, and/or networks. In accepting, collecting, and maintaining Plaintiff’s and the Class’s PII and PHI, Defendant agreed that they would protect and safeguard that data by complying with state and federal laws and regulations and applicable industry standards. Defendant was in possession of Plaintiff’s and the Class’s Private Information before, during, and after the Data Breach.

---

<sup>4</sup> <https://completecarenj.org/about-completecare-nj/notice-of-privacy-practices/> (last accessed February 5, 2024)

30. According to CCHN's Data Breach letters, it detected a "sophisticated ransomware attack" on or around October 12, 2023.<sup>5</sup>

31. In response, CCHN "disconnected the affected systems, initiated our response protocols, and engaged third-party forensic specialists to assist us with securing the network environment"<sup>6</sup> CCHN then determined that "the impacted data may have contained your personal information, including your name, phone number, address, social security number, and certain medical-related information."<sup>7</sup>

32. Beginning on or about December 15, 2023, over two months after the Data Breach began, Defendant finally and belatedly began notifying impacted third parties such as Plaintiff.

33. Despite Defendant's duties and commitments to safeguard sensitive and private information, Defendant failed to follow industry-standard practices in securing Plaintiff and the Class Members' Private Information, as evidenced by the Data Breach.

34. In response to the Data Breach, Defendant contends that it "began the process of securing and confirming the fortification of our systems." And that it has "taken steps to further secure our network and mitigate the risk of a similar incident occurring in the future, including revising our policies and procedures and network security software, and revising how we store and manage data."<sup>8</sup> It has not, however, addressed whether any of the data security flaws that contributed to the Data Breach have been remediated, nor has it identified what flaws in their

---

<sup>5</sup> <https://completecarenj.org/about-completecarenj/notice-of-cybersecurity-incident/> (last accessed February 5, 2024)

<sup>6</sup> *See id.*

<sup>7</sup> *See* Exhibit 1.

<sup>8</sup> *See* <https://completecarenj.org/about-completecarenj/notice-of-cybersecurity-incident/> (Last Accessed February 5, 2024)

policies, procedures, and network security software led to the data breach.<sup>9</sup> Nor do the Data Breach letters indicate the status of any law enforcement proceedings relating to the cybersecurity incident (beyond a mere statement that Federal law enforcement was “notified”), or any identification of whether the party responsible for the Breach has been identified or apprehended.

35. Defendant maintains a link on their website titled “Privacy Policy & Patient Rights.” However, the link Defendant provides does not appear to direct visitors to a functional page on Defendant’s website and instead returns a page indicating “No Results Found.”<sup>10</sup>

36. As of December 20, 2023, Defendant appears to have reported to Health and Human Services (HHS) that their Data Breach affected a total of 313,973 people.<sup>11</sup> Defendant’s Data Breach letters reveal that the following types of information were at a minimum compromised by the data breach: “personal information, including your name, phone number, address, social security number, and certain medical-related information.”<sup>12</sup> Notably, Defendant does not clarify precisely what other information may qualify as “personal information” nor what “medical-related information” may have been disclosed. This information is critically important to victims of a data breach, yet here victims such as Plaintiff are only told in very vague terms what data was breached.

37. Upon information and belief, the Private Information stored and maintained by Defendant was not encrypted.

---

<sup>9</sup> *Id.*

<sup>10</sup> See <https://completecarenj.org/patient-rights-policies/> (Last Accessed February 5, 2024)

<sup>11</sup> [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) (Last Accessed February 5, 2024)

<sup>12</sup> See Exhibit 1.



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

39. Upon information and belief, the cyberattack was targeted at Defendant due to its status as an entity that collects, creates, and maintains both PII and PHI.

40. Through its Data Breach notice letters to Plaintiff and Class Members, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach by encouraging victims “to remain vigilant by regularly monitoring your account statements and credit history for any signs of unauthorized transactions or activity.”<sup>13</sup>

41. Defendant’s response to the Data Brach does not adequately address the lifelong harm that victims will face following the Data Breach. The risk of identity theft and unauthorized use of Plaintiff and Class Members’ Private Information remains very high. The fraudulent activity resulting from the Data Breach may not come to light for years.

**C. Defendant Had a Duty to Secure Plaintiff and Class Members’ Private Information.**

42. As a regular and necessary part of their business, Defendant collected the highly sensitive Private Information of their patients.

43. Defendant had a duty to ensure that all information they collected and stored was secure, and that it maintained adequate and commercially reasonable data security practices to ensure the protection of Plaintiff and the Class Members’ Private Information.

44. Defendant is covered under the Health Insurance Portability and Accountability Act (“HIPAA”).

---

<sup>13</sup> *Id.*

45. As a covered entity, Defendant is required under federal and state law to maintain the strictest confidentiality of patients' Private Information that it acquires, receives, and collects. It is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

46. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

47. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

48. HIPAA requires that Defendant implement appropriate safeguards for this information.

49. HIPAA also requires Defendant to "review and modify the security measures implemented ... as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).

50. Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

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

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

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

54. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” *See* US Department of Health & Human Services, Security Rule Guidance Material. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, “represent the industry standard

for good business practices with respect to standards for securing e-PHI.” *See* US Department of Health & Human Services, Guidance on Risk Analysis.

**D. The Healthcare Sector Is Increasingly Susceptible to Data Breaches, Giving Defendant Notice That It Was a Likely Cyberattack Target**

55. At all relevant times, Defendant knew, or should have known, that the Private Information it was entrusted with was a target for malicious actors. Defendant knew this given the unique type and the significant volume of data on its networks, servers, and systems, comprising individuals’ detailed and confidential personal information and, thus, the significant number of individuals who the exposure of the unencrypted data would harm.

56. As custodian of Plaintiff’s and Class Members’ Private Information, Defendant knew or should have known the importance of protecting that information, and of the foreseeable consequences and harms to such persons if any data breach occurred.

57. Defendant was on notice that the FBI has been long concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that “[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII).”<sup>14</sup>

58. Defendant’s security obligations were especially important due to the substantial increase of cyberattacks and data breaches in recent years, particularly those targeting healthcare

---

<sup>14</sup> Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 20, 2014), <https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820>. (last accessed February 5, 2024)

businesses and other organizations like Defendant, which store and maintain large volumes of PII and PHI. These largescale cyberattacks are increasingly common and well-publicized. Through the end of November 2023, 640 largescale cyberattacks had targeted hospitals, health systems, and healthcare records in 2023, affecting more than 115 million people—making 2023 the “worst-ever year for breached healthcare records.”<sup>15</sup> With the surging number of such attacks targeting companies in the healthcare sector, Defendant knew or should have known that it was at high risk of cyberattack and should have taken additional and stronger precautions and preemptive measures.

**E. Defendant Breached Its Duties to Plaintiff and the Class Members and Failed to Comply with Regulatory Requirements and Industry Practices**

59. Because it was entrusted with sensitive Private Information, Defendant owed to Plaintiff and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII and PHI in their care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to their networks and systems.

60. Defendant also owed a duty to safeguard Private Information because it was on notice that it was handling highly valuable data and knew there was a significant risk it would be targeted by cybercriminals. Furthermore, Defendant knew of the extensive, foreseeable harm that would ensue for the victims of a data breach, and therefore also owed a duty to reasonably safeguard that information.

---

<sup>15</sup> November 2023 Healthcare Data Breach Report, The HIPAA Journal (Dec. 21, 2023), <https://www.hipaajournal.com/november-2023-healthcare-data-breach-report/>.

61. Security standards commonly accepted among businesses like Defendant that store Private Information include, without limitation:

- i. Maintaining a secure firewall configuration;
- ii. Monitoring for suspicious or irregular traffic to servers or networks;
- iii. Monitoring for suspicious credentials used to access servers or networks;
- iv. Monitoring for suspicious or irregular activity by known users;
- v. Monitoring for suspicious or unknown users;
- vi. Monitoring for suspicious or irregular server requests;
- vii. Monitoring for server requests for PII or PHI;
- viii. Monitoring for server requests from VPNs; and
- ix. Monitoring for server requests for Tor exit nodes.

62. The U.S. Federal Trade Commission (“FTC”) publishes guides for businesses for cybersecurity<sup>16</sup> and protection of PII which includes basic security standards applicable to all types of businesses.<sup>17</sup>

63. The FTC recommends that businesses:

- i. Identify all connections to the computers where sensitive information is stored.
- ii. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

---

<sup>16</sup> Start with Security: A Guide for Business, FTC (June 2015), *available at* <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

<sup>17</sup> Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), *available at* [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf).

- iii. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.
- iv. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.
- v. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.
- vi. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.
- vii. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

- viii. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.
- ix. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

64. As described further below, Defendant owed a duty to safeguard Private Information under several statutes, including the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act") and as a covered entity under HIPAA, to ensure that all information it received, maintained, and stored was secure. These statutes were enacted to protect Plaintiff and the Class Members from the type of conduct in which Defendant engaged, and the resulting harms Defendant proximately caused Plaintiff and the Class Members.

65. Under the FTC Act, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members. Under HIPAA, 42 U.S.C. § 1320d, and its implementing regulations, 45 C.F.R. §§ 160, *et seq.*, Defendant had a duty to securely store and maintain the Private Information of Plaintiff and Class Members which was collected in conjunction with receiving medical services.

66. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.



67. Defendant knew or should have known of their obligation to implement appropriate measures to protect patients' Private Information but failed to comply with the FTC's basic guidelines and other industry best practices, including the minimum standards set by the National Institute of Standards and Technology Cybersecurity Framework Version 1.1.<sup>18</sup>

68. Defendant's failure to employ reasonable measures to adequately safeguard against unauthorized access to PII and PHI constitutes an unfair act or practice as prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, as well as by state statutory analogs.

69. Defendant failed to use reasonable care in maintaining the privacy and security of Plaintiff and the Class Members' Private Information. If Defendant had implemented adequate security measures, cybercriminals could never have accessed the Private Information of Plaintiff and the Class Members, and the Data Breach would have either been prevented or much smaller in scope.

70. Specifically, Defendant breached their duty to exercise reasonable care by failing to implement and maintain adequate data security measures to safeguard Plaintiff and Class Members' Private Information, failing to encrypt or anonymize Private Information within their systems and networks, failing to monitor their systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge Private Information no longer necessary for their provision of healthcare services to their clients and customers, allowing unmonitored and unrestricted access to unsecured Private Information, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiff's and Class Member's Private Information. Additionally, Defendant breached their duty by utilizing outdated and ineffectual data security

---

<sup>18</sup> <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>.

measures, which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Defendant also violated their duties under the FTC Act and HIPAA.

71. Due to the sensitive nature of the Private Information accessed in the Data Breach, cybercriminals can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and the Class Members now and indefinitely in the future. As a result, Plaintiff and the Class Members have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

72. The Data Breach exposed Private Information that is both valuable and highly coveted on underground markets because it can be used to commit identity theft and financial fraud.

73. Identity thieves use such information to, among other things, gain access to bank accounts, social media accounts, and credit cards. Identity thieves can also use it to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government identification cards, or create "synthetic identities." Additionally, identity thieves often wait significant amounts of time—months or even years—to use the information obtained in data breaches because victims often become less vigilant in monitoring their accounts as time passes, therefore making the stolen information easier to use without detection. These identity thieves will also re-use stolen data, resulting in victims of one data breach suffering the effects of several cybercrimes from one instance of unauthorized access to their Private Information.

74. Victims of data breaches are much more likely to become victims of identity fraud than those who have not. Data Breach victims who do experience identity theft often spend hundreds of hours fixing the damage caused by identity thieves.<sup>19</sup>

75. Additionally, the U.S. Department of Justice Bureau of Justice Statistics has reported that, even if data thieves have not caused financial harm, data breach victims “reported spending an average of about 7 hours clearing up the issues.”<sup>20</sup>

76. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult to change. The Social Security Administration stresses that the loss of an individual’s Social Security number can lead to identity theft and extensive financial fraud:

Identity theft is one of the fastest growing crimes in America. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don’t pay the bills, it damages your credit. You may not find out that someone is using your number until you’re turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.

Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.<sup>21</sup>

77. The information compromised in the Data Breach—including Social Security numbers—is much more valuable than the loss of credit card information in a retailer data breach. There, victims can simply close their credit and debit card accounts and potentially even rely on automatic fraud protection offered by their banks. Here, however, the information

---

<sup>19</sup> <https://www.marylandattorneygeneral.gov/ID%20Theft%20Documents/Identitytheft.pdf>.

<sup>20</sup> <https://bjs.ojp.gov/content/pub/pdf/vit14.pdf>.

<sup>21</sup> Social Security Administration, Identity Theft and Your Social Security Number <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Jan. 22, 2024).

compromised is much more difficult, if not impossible, for consumers to resecure after being stolen. And it includes some of the most highly personal and sensitive health information.

**F. Defendant Failed to Provide Adequate Notice of the Data Breach.**

78. The law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of Private Information to Plaintiff and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information.

79. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires HIPAA covered entities and their business associates, like Defendant, to provide notification following a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons— i.e. non-encrypted data—to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach.*” (emphasis added)

80. Should a health care provider experience an unauthorized disclosure, it is required to conduct a risk assessment under HIPAA, as follows: “A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported.” The four-factor risk assessment focuses on: (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results); (2) the recipient of the PHI; (3) whether the PHI was actually acquired or viewed; and, (4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed).

81. Defendant detected the breach as early as October 23, 2023. However, Defendant did not notify Plaintiff Matczak of the breach until on or about December 27, 2023. This unreasonable delay in providing notice violated state and federal laws, including HIPAA, and further exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiff and Class Members.

**G. Plaintiff Matczak Was Harmed by the Data Breach.**

82. According to their notice letter, Defendant CCHN both obtained and disclosed Plaintiff Matczak's Private Information.<sup>22</sup>

83. Upon information and belief, Plaintiff Matczak was presented with standard forms to complete prior to receiving services that required her Private Information. Upon information and belief, Defendant received and maintained the information Plaintiff Matczak was required to provide to her doctors or medical professionals.

84. Plaintiff Matczak took reasonable steps to maintain the confidentiality of her Private Information. She relied on her healthcare providers, including Defendant, to keep her information secure and confidential.

85. As a result of the Data Breach, Plaintiff Matczak suffered actual injuries including: (a) paying money to her healthcare providers for services, which she would not have done had Defendant disclosed that they lacked data security practices adequate to safeguard her Private Information from theft; (b) damages to and diminution in the value of her Private Information—property that Plaintiff entrusted to Defendant; (c) loss and invasion of her privacy;

---

<sup>22</sup> Ex. 1.

and (d) injuries arising from the increased risk of fraud and identity theft, including the cost of taking reasonable identity theft protection measures, which will continue for years.

86. Plaintiff Matczak was also forced to take measures to mitigate the harm, including time monitoring her credit and financial accounts, researching the Data Breach, and researching and taking steps to prevent and mitigate further identity theft. Plaintiff Matczak also anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. Defendant's offer to provide one year of credit monitoring is entirely insufficient in light of the extended period of time the released data puts Plaintiff at risk and the ongoing costs and expenses associated with mitigation efforts.

87. Plaintiff Matczak has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

#### **H. Plaintiff and the Class Suffered Actual and Impending Injuries Resulting from the Data Breach**

88. Plaintiff and the Class Members face a lifetime of constant surveillance of their financial, personal, and health records; monitoring; loss of reputation; and loss of rights. Plaintiff and the Class are incurring and will continue to incur such damage in addition to any fraudulent use of their PII/PHI.

89. PII/PHI is very valuable to criminals, as evidenced by the prices they will pay for it on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For

example, personal information is sold at prices ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.<sup>23</sup>

90. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that “when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.”<sup>24</sup>

91. The information compromised in the Data Breach is significantly more valuable than the loss of, for example, payment card information in a retailer data breach because, in that situation, victims can cancel or close payment card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—name, birthdate, health insurance information, and health records.

92. Cyber criminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity.<sup>25</sup> The shelf life for this information is

---

<sup>23</sup> *Your Personal Data Is for Sale on the Dark Web. Here’s How Much It Costs*, Digital Trends (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs>.

<sup>24</sup> Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) <https://www.jstor.org/stable/23015560?seq=1>.

<sup>25</sup> *Medical Identity Theft: FAQs for Health Care Providers and Health Plans*, FTC, <https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf> (last visited February 5, 2024).

also much longer—while individuals can update their credit card numbers, they are less likely to change their Medicare numbers or health insurance information.

93. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to \$1,200 to \$1,300 each on the black market.<sup>26</sup> According to a report released by the Federal Bureau of Investigation’s (“FBI”) Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.<sup>27</sup>

94. Identity thieves may use stolen data to commit health care fraud, prescription drug fraud, bank fraud, credit card fraud, employer or tax-related fraud, government documents or benefits fraud, loan or lease fraud, phone or utilities fraud, among other forms of fraud.<sup>28</sup>

95. Criminals can use stolen PII/PHI to extort a financial payment by “leveraging details specific to a disease or terminal illness.”<sup>29</sup> Quoting Carbon Black’s Chief Cybersecurity Officer, one recent article explained: “Traditional criminals understand the power of coercion and extortion. ... By having healthcare information—specifically, regarding a sexually

---

<sup>26</sup> See SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG (July 16, 2013), <https://www.scmagazine.com/news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market>.

<sup>27</sup> See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (Apr. 8, 2014), <https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systemscyber-intrusions.pdf>.

<sup>28</sup> FTC Consumer Sentinel Network, *Compare Identity Theft Report Types*, <https://public.tableau.com/app/profile/federal.trade.commission/viz/IdentityTheftReports/TheftTypesOverTime>, (Last visited February 5, 2024).

<sup>29</sup> See Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcaredata-perfcon> (“What Happens to Stolen Healthcare Data”) (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating “Health information is a treasure trove for criminals.”).



transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do.”<sup>30</sup>

96. Cybercriminals can take the PII/PHI of Plaintiff and the Class Members to engage in identity theft, healthcare fraud, and/or to sell it to other criminals who will purchase the PII/PHI for that purpose. The fraudulent activities resulting from the Data Breach may not come to light for years.

97. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person’s name.<sup>31</sup>

98. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose job opportunities or be denied loans for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

99. Identity theft, which costs Americans billions of dollars annually, occurs when an individual’s PII is used without consent to commit fraud or other crimes. Victims of identity theft typically lose hundreds of hours dealing with the crime and hundreds, if not thousands, of dollars.

100. According to Javelin Strategy & Research, in 2018 alone, identity theft affected over 16.7 million individuals, causing a loss of over \$16.8 billion.

---

<sup>30</sup> *Id.*

<sup>31</sup> See Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM’N CONSUMER INFO.

101. Recent FTC data reveals that identify theft remains the top category of fraud reports received by the agency.<sup>32</sup> The FTC received over 1,100,000 reports of identity theft in 2022, and over 280,000 for the first quarter of 2023 alone.<sup>33</sup>

102. Identity thieves use personal information for various crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.<sup>34</sup> According to Experian, one of the largest credit reporting companies in the world, “[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it” to, among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver’s license or ID; or use the victim’s information in the event of arrest or court action.<sup>35</sup>

103. With access to an individual’s PII, criminals can do more than just empty a victim’s bank account. They can also commit all manner of fraud, including (i) obtaining a driver’s license or official identification card in the victim’s name but with the thief’s picture; (ii)

---

<sup>32</sup> FTC Consumer Sentinel Network, Federal Trade Commission, <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudandIDTheftMaps/AllReportsbyState>, (Last visited February 5, 2024).

<sup>33</sup> *Id.*

<sup>34</sup> The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 12 C.F.R. § 1022.3(h). The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” 12 C.F.R. § 1022.3(g).

<sup>35</sup> See Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN,, <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/> (last accessed February 7, 2024).

using the victim's name and SSN to obtain government benefits; or (iii) filing a fraudulent tax return using the victim's information. In addition, identity thieves may even give the victim's personal information to police during an arrest.<sup>36</sup>

104. Consumers place a high value not only on their personal information but also on the privacy of that data. They do so because identity theft causes “significant negative financial impact on victims” in addition to severe distress and other strong emotional and physical reactions.

105. The United States Government Accountability Office (“GAO”) explains that “[t]he term ‘identity theft’ is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else’s name.”<sup>37</sup> The GAO Report notes that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”<sup>38</sup>

106. Further, as noted, there is the likelihood of a lapse in time between when the harm occurs to a victim of identity theft and when that harm is discovered, as well as a lapse between when the PII/PHI is stolen and when it is actually used. According to the GAO, which conducted a study regarding the growing number of data breaches:

---

<sup>36</sup> See Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last accessed Mar. 21, 2023); See Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RES.

<sup>37</sup> See Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, U.S. Government Accountability Office Report to Congressional Requesters (“GAO Report”) at 2 (June 2007), <https://www.gao.gov/new.items/d07737.pdf>, (Last visited February 7, 2024).

<sup>38</sup> *Id.*

107. Further, as noted, there is the likelihood of a lapse in time between when the harm occurs to a victim of identity theft and when that harm is discovered, as well as a lapse between when the PII/PHI is stolen and when it is actually used. According to the GAO, which conducted a study regarding the growing number of 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.<sup>39</sup>

108. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than \$3.5 billion in losses to individuals and business victims.<sup>40</sup>

109. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."<sup>41</sup> Defendant did not rapidly or timely report to Plaintiff and the Class Members that their Private Information had been stolen.

110. As a result of the Data Breach, Plaintiff and the Class Members' Private Information has been exposed to criminals for misuse. The injuries suffered by Plaintiff and the Class Members, or likely to be suffered thereby as a direct result of the Data Breach, include:

- a. unauthorized use of their PII/PHI;

---

<sup>39</sup> See GAO Report, at p.29.

<sup>40</sup> 2019 Internet Crime Report Released, FBI, <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion.> (Last visited February 7, 2024).

<sup>41</sup> *Id.*

- b. theft of their personal, financial, and health information;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial and healthcare accounts;
- d. damages arising from the inability to use their PII/PHI;
- e. improper disclosure of their PII/PHI;
- f. loss of privacy and embarrassment;
- g. loss of reputation;
- h. trespass and damage to their personal property, including PII/PHI;
- i. the imminent and certainly impending risk of having their confidential medical information used against them by spam callers and/or hackers targeting them with phishing schemes to defraud them;
- j. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;
- k. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII/PHI being placed in the hands of criminals and already misused via the sale of Plaintiff and the Class Members' information on the Internet black market; and
- l. damages to and diminution in value of their PII/PHI entrusted to Defendant.

111. In addition to a remedy for economic harm, Plaintiff and the Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

112. Defendant disregarded the rights of Plaintiff and the Class Members by (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions; (ii) failing to disclose that Defendant did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff and the Class Members' Private Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; and (iv) failing to provide Plaintiff and the Class Members prompt notice of the Data Breach.

113. The actual and adverse effects to Plaintiff and the Class Members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud, and medical fraud directly or proximately caused by Defendant's wrongful actions or inaction and the resulting Data Breach require Plaintiff and the Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes, and closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and the Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

### **CLASS ACTION ALLEGATIONS**

114. Plaintiff brings this action as a class action pursuant to Rules 23(a) and 23(b)(1)-(3) of the Federal Rules of Civil Procedure, on behalf of herself and a Class, defined as follows:

All persons in the United States whose Private Information was compromised in the Data Breach announced by CCHN in December 2023, including all who were sent a notice of the Data Breach.

115. Excluded from the Class are governmental entities, Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns. Also excluded are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

116. This action is brought and may be properly maintained as a class action pursuant to Rule 23. This action satisfies the requirements of Rule 23, including numerosity, commonality, typicality, adequacy, predominance, and superiority.

117. **Numerosity.** The Class is so numerous that the individual joinder of all members is impracticable. While the Class Members' exact number are currently unknown and can only be ascertained through appropriate discovery, Defendant purports to provide services to over 60,000 people per year.

118. **Commonality.** Common legal and factual questions exist that predominate over any questions affecting only individual Class Members. These common questions, which do not vary among Class Members and which may be determined without reference to any Class member's individual circumstances, include, but are not limited to:

- a. Whether Defendant knew or should have known that its systems were vulnerable to unauthorized access;

- b. Whether Defendant failed to take adequate and reasonable measures to ensure its data systems were protected;
- c. Whether Defendant failed to take available steps to prevent and stop the breach from happening;
- d. Whether Defendant owed a legal duty to Plaintiff and Class Members to protect their Private Information;
- e. Whether Defendant breached any duty to protect the personal information of Plaintiff and Class Members by failing to exercise due care in protecting their Private Information;
- f. Whether Defendant breached any implied contracts;
- g. Whether Defendant was unjustly enriched by its actions;
- h. Whether Plaintiff and Class Members are entitled to actual, statutory, or other forms of damages and other monetary relief, and the extent of such damages and relief, and;
- i. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief or restitution and the extent of such damages and relief.

119. **Typicality.** Plaintiff's claims are typical of other Class Members' claims because Plaintiff and the Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.

120. **Adequacy of Representation.** Plaintiff is an adequate Class representative because she is a Class member, and her interests do not conflict with the Class's interests. Plaintiff retained counsel who are competent and experienced in class action and data breach



litigation. Plaintiff and her counsel intend to prosecute this action vigorously for the Class's benefit and will fairly and adequately protect their interests.

121. **Predominance and Superiority.** The Class can be properly maintained because the above common questions of law and fact predominate over any questions affecting individual Class Members.

122. A class action is also superior to other available methods for the fair and efficient adjudication of this litigation because individual litigation of each Class member's claim is impracticable. Even if each Class member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common legal and factual questions. By contrast, the class-action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

123. **Declaratory and Injunctive Relief.** The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class Members and impair their interests. Defendant has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

## **CLAIMS FOR RELIEF**

### **CLAIM I**

#### **Negligence**

#### ***On behalf of Plaintiff and the Class Against Defendant***

124. Plaintiff incorporates by reference and realleges each allegation in paragraphs 1 to 123 as though fully set forth herein.

125. In order to receive medical treatments and services, Plaintiff and Class Members were required to provide non-public Private Information, such as PII and PHI, to Defendant.

126. Plaintiff and Class Members entrusted their Private Information to Defendant with the understanding that Defendant would safeguard their information.

127. However, it appears hundreds of thousands of patients (including Plaintiff) had sensitive data “shared” with hackers without their knowledge or consent.

128. Defendant did not take reasonable and appropriate safeguards to protect Plaintiff and Class Members’ Private Information.

129. Defendant had full knowledge of the sensitivity of the Private Information that they stored and the types of harm that Plaintiff and Class Members could and would suffer if that Private Information were wrongfully disclosed.

130. Defendant violated their duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and testing Defendant’s information security controls sufficiently rigorously to ensure that PII and PHI in their possession was adequately secured by, for example, encrypting sensitive personal information, installing effective intrusion detection systems and monitoring mechanisms, using access controls to limit access to sensitive data, regularly testing for security weaknesses and

failures, failing to notify customers of the breach in a timely manner, and failing to remedy the continuing harm by unreasonably delaying notifying specific victims who were harmed.

131. Defendant's duty of care arose from, among other things,

- a. Defendant's exclusive ability (and Class Members' inability) to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur;
- b. Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures;
- c. Defendant's common law duties to adopt reasonable data security measures to protect Private Information and to act as a reasonable and prudent person under the same or similar circumstances would act; and
- d. State statutes requiring reasonable data security measures.

132. Defendant's violation of the FTC Act and HIPAA constitutes negligence per se for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the types of harm that resulted from the Data Breach.

133. Defendant had the financial and personnel resources necessary to prevent the Data Breach. Defendant nevertheless failed to adopt reasonable data security measures, in breach of the duties they owed to Plaintiff and Class Members.

134. Plaintiff and Class Members were the foreseeable victims of Defendant's inadequate data security. Defendant knew that a breach of their systems could and would cause harm to Plaintiff and Class Members.

135. Defendant's conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's conduct included their failure to adequately mitigate harm through negligently failing to inform patients and victims of the breach for over ten months after the purported first discovery of suspicious activity and eight months after criminals publicly announced that they had breached Defendant's systems.

136. Defendant knew or should have known of the inherent risks in collecting and storing massive amounts of Private Information, the importance of providing adequate data security over that Private Information, and the frequent cyberattacks within the medical industry.

137. Defendant through their actions and inactions, breached their duty owed to Plaintiff and Class Members by failing to exercise reasonable care in safeguarding their Private Information while it was in their possession and control. Defendant breached their duty by, among other things, their failure to adopt reasonable data security practices and their failure to adopt reasonable security and notification practices to prevent the Data Breach, including monitoring internal systems and sending notifications to affected victims. Defendant failed to notice suspicious activities during February through April 2023 and failed to implement sufficiently stringent security measures.

138. Defendant inadequately safeguarded patients' Private Information in breach of standard industry rules, regulations, and best practices at the time of the Data Breach.

139. But for Defendant's breach of their duty to adequately protect Class Members' Private Information, Class Members' Private Information would not have been stolen.

140. There is a temporal and close causal connection between Defendant's failure to implement adequate data security measures and notification practices, the Data Breach, and the harms suffered by Plaintiff and Class Members.

141. As a result of Defendant's negligence, Plaintiff and Class Members suffered and will continue to suffer the damages alleged herein.

142. Plaintiff and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate identity protection services. Plaintiff and Class Members are also entitled to the injunctive relief sought herein.

**CLAIM II**  
**Breach of Implied Contract**  
***On behalf of Plaintiff and the Class Against Defendant***

143. Plaintiff incorporates by reference and realleges each allegation in paragraphs 1 to 142 as though fully set forth herein.

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

145. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when she first utilized Defendant's services.

146. The valid and enforceable implied contracts to provide medical services that Plaintiff and Class Members entered into with Defendant or their customers include the promise to protect non-public Private Information given to Defendant (or that Defendant created on their own) from disclosure.

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

148. Defendant and/or their agents solicited 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.

149. 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.

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

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

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

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

154. Defendant's representations memorialize and embody the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff and Class Members' Private Information.

155. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To patients such as the Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiff and Class Members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected. 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 they adopted reasonable data security measures.

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

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

158. Defendant materially breached its contractual obligation to protect the non-public Private Information that Defendant collected when Plaintiff and Class Members' Private Information was accessed by unauthorized personnel as part of the Data Breach.

159. Defendant materially breached the terms of the implied contracts. Defendant did not maintain the privacy of Plaintiff and Class Members' Private Information as evidenced by its notification of the Data Breach to Plaintiff and at least tens of thousands of Class Members.

160. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiff and the Class Members' Private Information, as set forth above.

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

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

**CLAIM III**  
**Unjust Enrichment**  
*On behalf of Plaintiff and the Class Against All Defendant*

163. Plaintiff incorporates by reference and realleges each allegation in paragraphs 1 to 123 above as though fully set forth herein.

164. This claim is plead in the alternative to the breach of contract count above.

165. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant 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.



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

167. The amounts Plaintiff and Class Members paid for goods and services were used, in part, to pay for use of Defendant's costs of data management and security.

168. 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.

169. 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 to Defendant.

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

171. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to Defendant's services.

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

173. 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 fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs, including the time, effort, and money that will be expended to prevent, detect, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of Plaintiff and Class Members' lives.

174. 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 harm.

175. 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 Plaintiff and Class Members. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of herself and the Class set forth herein, respectfully requests the following relief:

- A. Certifying this action as a class action under Fed. R. Civ. P. 23 and appointing Plaintiff and her counsel to represent the Class;
- B. Entering judgment for Plaintiff and the Class;
- C. Granting permanent and appropriate injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described

herein and directing Defendant to adequately safeguard the Private Information of Plaintiff and the Class by implementing improved security controls;

- D. Awarding compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;
- E. Awarding statutory or punitive damages and penalties as allowed by law in an amount to be determined at trial;
- F. Ordering disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of their unlawful acts, omissions, and practices;
- G. Awarding to Plaintiff and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;
- H. Awarding pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper; and
- I. Granting such further and other relief as may be just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands a jury trial on all claims so triable.

Dated: February 8, 2024

Respectfully submitted,

/s/ Natalie Finkelman Bennett

James C. Shah

Natalie Finkelman Bennett

**MILLER SHAH LLP**

2 Hudson Place, Suite 100

Hoboken, NJ 07030

Tel: (866) 540-5505

Fax: (866) 300-7367

jcshah@millershah.com

nfinkelman@millershah.com

Amber L. Schubert (*pro hac vice* to be filed)

**SCHUBERT JONCKHEER & KOLBE LLP**

2001 Union St., Suite 200

San Francisco, CA 94123

Tel: (415) 788-4220

Fax: (415) 788-0161

aschubert@sjk.law

*Counsel for Plaintiff*