UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK
MANHATTAN DIVISION

SARAH HAMM, individually and on behalf of themselves and all others similarly situated,

Plaintiff,

v.

CAPSULE CORPORATION d/b/a CAPSULE, a Delaware Corporation;

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff (the "Plaintiff"), on behalf of herself and all others similarly situated, alleges the following Class Action Complaint (the "Action") against the above-captioned Defendant ("Defendant") upon personal knowledge as to herself and her own actions, and upon information and belief, including the investigation of counsel as follows:

I. INTRODUCTION

1. Defendant Capsule Corporation d/b/a Capsule (hereinafter, "Capsule") is an online and mobile application-based pharmacy "that delivers your prescriptions, the same day, for free – all from your phone."[1]

2. On or about May 27, 2022, Capsule posted or caused to post a notice, entitled "Notice of Security Incident" (hereinafter, the "Notice") with the California Attorney General's office, announcing publicly that "unauthorized threat actors gained access to certain Capsule accounts."[2]

3. This is despite the fact that Capsule, an online pharmacy, represents on its online webpage, amongst other representations: "**Your information is always secure with us**. **We store all of your personal data in an encrypted, HIPAA-compliant environment**."[3]

4. According to Capsule's Notice, customers of Capsule's pharmacy had their personally identifiable information ("PII") and protected health information ("PHI"), as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), compromised; this PII and PHI includes: patient demographic information (name, email address, phone number, physical address, date of birth, and sex), health information (medical conditions and prescribed medications), past order history [of medications through Capsule], payment information (last four

[1] www.capsule.com, (last accessed June 21, 2022).
[2] https://oag.ca.gov/system/files/Individual%20Notice%20Template_3.pdf, (last accessed June 21, 2022).
[3] https://www.capsule.com/questions, (last accessed June 22, 2022)(emphasis added).

digits of credit card/debit card and expiration date), insurance information (group ID and policyholder ID), as well as the text of chat message conversations with Capsule's staff, agents, and other personnel (collectively, the "Private Information).[4] This Private Information was accessed and compromised by an unauthorized threat actor in the cybersecurity incident (hereinafter, the "Data Breach").

5. As detailed below, the Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's and the Class Members' Private Information despite the fact that data breach attacks against medical systems and healthcare providers are at an all-time high.

6. This attack enabled an unauthorized third-party to access Defendant's computer systems and the highly sensitive and confidential data of over 27,000 customers of Capsule, including Plaintiff.

7. Plaintiff received a notification letter (the Notice) from Defendant informing her that the information accessed by the third-party actors included her electronic health records.

8. Capsule, despite professing to take the privacy and security of its customers confidential and health information seriously, has not offered to provide affected individuals with adequate credit monitoring service or compensation for the damages they have suffered as a result of the Data Breach.

9. Additionally, despite Capsule professing to take the privacy and security of its customers confidential and health information seriously, Capsule omits several key details from its Notice letter: (1) the method in which the unauthorized threat actors gained access to Capsule's computer network and/or data; (2) how long the unauthorized threat actors had access to Capsule's

[4] *Id.*

computer network and/or data; (3) the amount of time it took for Capsule to conduct its investigation, and (4) the amount of time that it took for Capsule to eliminate the unauthorized access of Plaintiff's and Class Members' Private Information.

10. As a consequence of the Data Breach, Plaintiff's and Class members' Private Information has been released into the public domain and they have had to, and will continue to have to, spend time to protect themselves from fraud and identity theft.

11. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, through frequent news reports and FBI warnings to the healthcare industry, and thus it was on notice that failing to take steps necessary to secure the Private Information from those risks left the property in a dangerous and vulnerable condition.

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

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

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

15. Plaintiff and Class Members 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.

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

17. Plaintiff seeks remedies including, but not limited to, all forms of allowable damages, including statutory damages, compensatory damages, nominal damages, reimbursement of out-of-pocket costs; injunctive relief including improvements to Defendant's data security systems, future annual audits; and adequate credit monitoring services funded by Defendant.

II. JURISDICTION AND VENUE

18. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and Plaintiff, a resident of Los Angeles, California, is a citizen of a state different from Defendant, incorporated in Delaware and headquartered in New York, to establish minimal diversity.

19. The Southern District of New York has personal jurisdiction over Defendant named in this action because Defendant is headquartered in this District and conducts substantial business in New York and this District through its headquarters, offices, and affiliates.

20. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District and has caused harm to Plaintiff and Class Members residing in this District.

III. PARTIES

Plaintiff Sarah Hamm

21. Plaintiff Sarah Hamm is a resident of the State of California and intends to remain domiciled in and a resident of the State of California. Plaintiff received the Notice on or about May 27, 2022. Plaintiff was informed that her sensitive Private Information was compromised in the Data Breach.

Defendant Capsule Corporation

22. Defendant Capsule Corporation d/b/a Capsule is a Delaware corporation which maintains its principal place of business in New York, New York.

IV. FACTUAL ALLEGATIONS

Defendant's Business

23. Capsule is an online and mobile application-based pharmacy.

24. When Capsule was founded, the "startup's aim is to build a "one-stop-shop" for digital healthcare where consumers access Capsule's digital pharmacy with a curated set of products and services – such as telemedicine or mental health support – all from within a single app."[5]

25. Since Capsule's founding in 2015, Capsule raised $570 million in financing and funding through the first six months of 2021.[6]

[5] Heather Landi, "*Digital pharmacy startup Capsule clinches $300M to invest in 'one-stop-shop' for digital health,*" FIERCE HEALTHCARE (ONLINE)(Apr. 28, 2021), at https://www.fiercehealthcare.com/tech/digital-pharmacy-startup-capsule-clinches-300m-to-invest-one-stop-shop-for-digital-healthcare.
[6] *Id.*

26. Capsule's "Capsule Privacy Policy" (hereinafter, the "Policy"), effective on October 8, 2021, which was prior to the Data Breach, states "Capsule is committed to safeguarding the privacy and security of the information that you provide to us or that others provide to us on your behalf."[7] Capsule also states in their website's Frequently Asked Questions, which are often a basis for consumers when evaluating whether or not to use a service or to purchase a good (especially online):

a. "Is my information secure? **Your information is always secure with us**. **We store all of your personal data in an encrypted, HIPAA-compliant environment**."[8]

27. Plaintiff read and relied on the Capsule Privacy Policy when she made her decision to transact with Defendant. Defendant's representations concerning privacy and data security were material information to Plaintiff. Had Plaintiff known of the true state of Defendant's privacy ad security practices, she either would not have transacted with Defendant at all or would have paid less for the services. Plaintiff would consider doing business with Defendant in the future if she could rely on their representations concerning their privacy and security practices.

28. Unfortunately, the Private Information of Plaintiff and the Class Members was not secure, was not encrypted, and was not kept in a HIPAA-compliant manner.

29. Additionally, Policy fails to state exactly what PII and PHI that they collect from their customers.

30. In the ordinary course of receiving health care services from Capsule, customers are required to provide, at a minimum, the Private Information, which is the data set of information compromised in this Data Breach, as previously stated: patient demographic information (name, email address, phone number, physical address, date of birth, and sex), health information (medical

[7] https://www.capsule.com/privacy, (last accessed June 22, 2022).
[8] https://www.capsule.com/questions, (last accessed June 22, 2022)(emphasis added).

conditions and prescribed medications), past order history [of medications through Capsule], payment information (last four digits of credit card/debit card and expiration date), insurance information (group ID and policyholder ID), as well as the text of chat message conversations with Capsule's staff, agents, and other personnel.

31. Prior to receiving care and treatment from Capsule, Plaintiff was required to and did in fact turn over much (if not all) of the private and confidential information listed above.

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

33. Capsule also likely creates and maintains a considerable amount of Protected Health Information (PHI) in the course of providing medical care and treatment. This PHI includes billing account numbers, financial information, medical record numbers, dates of service, provider names, and medical and clinical treatment information regarding care received from Capsule.

34. Capsule provides each of its patients with a HIPAA compliant notice of its privacy practices (the "Privacy Notice") in respect to how they handle patients' sensitive and confidential information.

35. A copy of the Privacy Notice is maintained on Capsule's website, and may be found here: https://www.capsule.com/hipaa.

36. Due to the highly sensitive and personal nature of the information Capsule acquires and stores with respect to its patients, Capsule recognizes patients' Rights to Privacy in its Privacy Notice, and promises in its Privacy Notice, to, among other things, maintain the privacy of patients' protected health information, which includes the types of data compromised in this Data Breach.

37. Capsule promises to maintain the confidentiality of patients' health, financial, and non-public personal information, ensure compliance with federal and state laws and regulations, and not to use or disclose patients' health information for any reasons other than those expressly listed in the Privacy Notice without written authorization.

38. As a condition of receiving medication from Defendant, Defendant requires that its patients entrust it with highly sensitive personal information.

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

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

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

The Data Breach

42. The Notice states, "[o]n April 5, 2022, unauthorized threat actors gained access to certain Capsule accounts. We discovered the issue on the same day and immediately began an investigation with the assistance of a third-party forensic firm. Through that investigation, we identified your account as potentially compromised."

43. The Notice then lists out the aforementioned Private Information as the information that "may" have been affected.[9]

[9] *Id.*

44. Although the Notice states that Defendant was the victim of a data security incident beginning on April 5, 2022, it provides scant detail about the nature, severity, or duration of the attack. Even worse, Defendant did not cause a Notice of Security Incident to be posted on its website or for the Notice(s) to be disseminated until over six weeks after Defendant first became cognizant of the Data Breach on April 5, 2022.

45. But what's clear from the Notice is that cybercriminals did, in fact, access and view Plaintiff's and Class members' PII and PHI during the time period in which the cybercriminals had unfettered access to Defendant's IT network, as that is the modus operandi of cybercriminals who commit such attacks.

46. Simply, Defendant could have prevented this Data Breach.

47. Defendant did not implement or maintain adequate measures to protect its patients' PII and PHI.

48. On information and belief, the PII and PHI compromised in the files accessed by hackers was not encrypted.

49. Moreover, the removal of PHI and other PII and PHI from Defendant's system demonstrates that this cyberattack was targeted due to Defendant's status as a healthcare facility that houses sensitive PII and PHI.

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

51. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of PII and PHI, Defendant provided unreasonably deficient protections prior to the Breach, including, but not limited to a lack of security measures

for storing and handling patients' PII and PHI and inadequate employee training regarding how to access, handle and safeguard this information.

52. Defendant failed to adequately adopt and train its employees on even the most basic of information security protocols, including: storing, locking encrypting and limiting access to patients' highly sensitive PHI; implementing guidelines for accessing, maintaining and communicating sensitive PHI, and protecting patients' sensitive PHI by implementing protocols on how to utilize such information.

53. Defendant's failures caused the unpermitted disclosure of Plaintiff's and Class members' Private Information to an unauthorized third party and put Plaintiff and the Class at serious, immediate and continuous risk of identity theft and fraud.

54. The Data Breach that exposed Plaintiff's and Class members' PHI was caused by Defendant's violation of its obligations to abide by best practices and industry standards concerning its information security practices and processes.

55. Defendant failed to comply with security standards or to implement security measures that could have prevented or mitigated the Breach.

56. Defendant failed to ensure that all personnel with access to its patients' PII and PHI were properly trained in retrieving, handling, using and distributing sensitive information.

The Breach Was Foreseeable

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

58. Plaintiff and Class members provided their PII and PHI 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.

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

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

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

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

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

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

65. In 2021 alone there were over 220 data breach incidents.

66. These approximately 220 data breach incidents have impacted nearly 15 million individuals.

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

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

69. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."

70. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across U.S. healthcare organizations. Significant security incidents are a near-universal experience in U.S. healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets."

71. PII and PHI is of great value to hackers and cybercriminals, and the data compromised in the Breach can be used in a variety of unlawful manners.

72. PII and PHI can be used to distinguish, identify or trace an individual's identity, such as their name and medical records.

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

74. Given the nature of this Data Breach, it is foreseeable that the compromised PII and PHI can be used by hackers and cybercriminals in a variety of different ways.

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

76. 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, upon information and good faith belief, to the Defendant.

Defendant Failed to Follow FTC Guidelines

77. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

78. According to the FTC, the need for data security should be factored into all business decision-making.

79. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

80. 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.

81. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

82. 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.

83. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

84. 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.").

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

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

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

Defendant Failed to Meet Industry Standards

88. 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.

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

90. 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.

91. 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.

92. 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 Breach.

Defendant Failed to Comply with HIPAA

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

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

95. Title II of HIPAA contains what are known as the Administrative Simplification provisions. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI and PII like the data Defendant left unguarded.

96. 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).

> A data breach such as the one Defendant experienced, is also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule: A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

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

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

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

Defendant's Breach

99. Defendant breached its obligations to Plaintiff and the Class members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, network and data.

100. 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 consumers' PHI and other PII and PHI;

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

d. Failing to apply all available security updates;

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

f. Failing to practice the principle of least-privilege and maintain credential hygiene; Failing to avoid the use of domain-wide, admin-level service accounts;

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

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

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

j. 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);

k. 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);

l. 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);

m. 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);

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

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

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

q. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key," 45 CFR § 164.304 (definition of encryption).

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

102. Accordingly, as outlined below, Plaintiff and Class members now face a substantial, increased, and immediate risk of fraud and identity theft.

Data Breaches Are Disruptive and Harm Consumers

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

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

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

106. 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."

107. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it.

108. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

109. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number.

110. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

111. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[11]

112. Theft of PII and PHI is gravely serious. PII and PHI is an extremely valuable property right.

113. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII and PHI has considerable market value.

114. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[14]

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

116. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when PII, PHI, and/or financial information is stolen and when it is used.

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm. See GAO Report, at p. 29.

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

119. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

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

121. Sensitive PII and PHI can sell for as much as $363 per record according to the Infosec Institute.

122. PII is particularly valuable because criminals can use it to target victims with frauds and scams.

123. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

124. Medical information is especially valuable to identity thieves.

125. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.

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

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

Harm to Plaintiff

128. On or about May 27, 2022, Plaintiff received notice from Defendant that her Private Information had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff's Private Information was compromised as a result of the Data Breach.

129. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff has spent several hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

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

and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

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

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

133. Because Plaintiff's and Class Member's sensitive data remains with Defendant it remains vulnerable to future unauthorized access and exfiltration absent Defendant implementing more robust security standards.

Plaintiff Has Met the Fraud Pleading Standard Under F.R.C.P. Rule 9(b)

134. Rule 9(b) of the Federal Rules of Civil Procedure provide that "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake. Although Defendant is in the best position to know what content they placed on their website and on other marketing materials during the relevant timeframe, to the extent necessary, as detailed in the paragraphs above and below, Plaintiff has satisfied the requirements of Rule 9(b) by establishing the following elements with sufficient particularity:

135. **WHO:** Defendant is the party who made material misrepresentations and/or omissions of fact in their uniform website representations, their Privacy Policy, and other

marketing materials when they misrepresented their privacy standards during the relevant timeframe.

136. **WHAT:** Defendant specifically made the following misrepresentations:

a. From the Defendant's website's FAQ: "Is my information secure? **Your information is always secure with us**. **We store all of your personal data in an encrypted, HIPAA-compliant environment**."[10]

b. From the Defendant's Privacy Policy: "**Capsule is committed to safeguarding the privacy and security of the information that you provide to us or that others provide on your behalf**."[11]

c. From the Defendant's website's homepage: "Privately chat or text with our expert pharmacists."[12]

137. These representations were false: (1) Plaintiff and Class Members' information was not "always" secure in the possession of Capsule; (2) Plaintiff and Class Members' data was not encrypted; (3) Plaintiff and Class Members' data was not stored in a "HIPAA compliant environment"; (4) Capsule is not "committed to safeguarding the privacy and information" that Plaintiff and Class Members' provided to them – they failed to even take basic measures to protect Plaintiff and Class Members' Private Information; (5) Plaintiff and Class Members' private chat/text conversations were exposed in the Data Breach – thus, these conversations are not (and were not) private.

[10] https://www.capsule.com/questions, (last accessed June 22, 2022)(emphasis added).
[11] https://www.capsule.com/privacy, (last accessed June 22, 2022)(emphasis added).
[12] https://www.capsule.com, (last accessed June 22, 2022).

138. **WHEN:** Defendant made these misrepresentations during the Class Period (as defined below) and continues to make these representations at the time of the filing of this Class Action Complaint.

139. **WHERE:** Defendant made these misrepresentations toward consumers throughout the entire United States (and potentially globally).

140. **HOW:** Defendant made these misrepresentations through their website and via their Privacy Policy.

141. **WHY:** Defendant made these misrepresentations because they know that consumers value their data and that consumers would not use Capsule had they known Capsule had woefully insufficient data security protections in place over their Private Information.

142. **INJURY:** Plaintiff and the Class Members were harmed in the following ways: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

The Agreements Made Between Plaintiff and Defendant Are Unenforceable

A. Plaintiff Was Fraudulently Induced

143. No agreement ("Agreement") exists, therefore, between the Plaintiff and the Defendant – and no Agreements exist between the Class Members and the Defendant – because Capsule deceived and fraudulently induced its consumers to enter into relationships with it for the provision of medication and other telehealth services.

B. Plaintiff's Claims Are Not Arbitable

144. Plaintiff and Class Members claims are not arbitrable because the Agreement that the Plaintiff and Class Members entered into with Defendant either were entered into fraudulently.

C. Alternatively, Plaintiff and Class Members' Claims Are Subject to Equitable and Injunctive Relief

145. Alternatively, if this Court were to find that an Agreement does exist – the operative Agreement would be the Terms of Service linked both on Capsule's website and on their mobile application. Those Terms of Service state: "either party may bring a lawsuit solely for injunctive or equitable relief without first engaging in arbitration or the informal dispute-resolution process described[.]"[13]

V. CLASS ALLEGATIONS

146. This Action is properly maintainable as a Class Action.

147. Plaintiff brings this Action on behalf of herself and all similarly situated persons and entities pursuant to Federal Rule of Civil Procedure 23, for the following Class and Subclass defined as:

> **National Class.** All individuals and entities residing in the United States whose PII and PHI was compromised on the Data Breach first announced by the Defendant in May of 2022.

[13] https://www.capsule.com/terms, (last accessed June 22, 2022).

California Subclass. All individuals and entities residing in the state of California whose PII and PHI was compromised on the Data Breach first announced by the Defendant in May of 2022.

(collectively, the "Class").

148. Excluded from the Classes are: Defendant and Defendant's relatives, subsidiaries, affiliates, officers and directors, and any entity in which the Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

149. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

150. Numerosity. Defendant reports that the Data Breach compromised PHI of 27,000+ consumers. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

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

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

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

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

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

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

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

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

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

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

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

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

152. Typicality. Plaintiff's claims are typical of those of other Class members because Plaintiff's PHI, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiff, like all Class members, was injured by Defendant's uniform conduct. Plaintiff are advancing the same claims and legal theories on behalf of herself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

153. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Class in that they has no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiff suffered are typical of other Class members, and Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class. Plaintiff has retained counsel

experienced in complex consumer class action litigation, including, but not limited to, similar data breach class action litigation, and Plaintiff intends to prosecute this action vigorously.

154. Superiority of Class Action. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based on an identical set of facts. In addition, without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

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

156. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

157. Predominance. The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

158. This proposed class action does not present any unique management difficulties.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On behalf of the Nationwide Class)

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

160. Defendant required Plaintiff and the Class Members to submit non-public personal information in order to obtain medical services – specifically, prescription medication and other telehealth services.

161. The Class members are individuals who provided certain PII and PHI to Defendant including, and at a minimum, the Private Information described above.

162. Defendant had full knowledge of the sensitivity of the PII and PHI to which it was entrusted and the types of harm that Class members could and would suffer if the information were wrongfully disclosed.

163. Defendant had a duty to each Class member to exercise reasonable care in holding, safeguarding and protecting that information.

164. Plaintiff and the Class members were the foreseeable victims of any inadequate safety and security practices.

165. The Class members had no ability to protect their data in Defendant's possession.

166. By collecting and storing this data in its computer property, and by sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and the Class members' PII and PHI held within it — to prevent disclosure of the information and to safeguard the information from theft.

167. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

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

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

170. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, which is recognized by laws and regulations including, but not limited to, HIPAA, as well as the common law.

171. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

172. 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).

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

174. 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.

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

176. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Class members' PHI and PII.

177. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to adopt, implement and maintain adequate security measures to safeguard Class members' PII and PHI;

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

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

d. Allowing unauthorized access to Class members' PII and PHI;

e. Failing to detect in a timely manner that Class members' PII and PHI had been compromised;

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

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

178. It was foreseeable that Defendant's failure to use reasonable measures to protect Class members' PII and PHI would result in injury to Plaintiff and Class members.

179. Further, the breach of security was reasonably foreseeable given the known high frequency of hacking incidents, cyberattacks, and data breaches in the healthcare industry.

180. It was therefore foreseeable that the failure to adequately safeguard Class members' PII and PHI would result in one or more types of injuries to Class members.

181. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Breach.

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

SECOND CAUSE OF ACTION
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349
(On behalf of the Nationwide Class)

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

184. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members Private Information, which was a proximate and direct 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. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

d. Failing to timely and adequately notify the Plaintiff and Class Members of the Data Breach;

e. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class Members' Private Information; and

g. 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 Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

185. Defendant's representations and 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 consumers' Private Information.

186. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers.

187. Defendant acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and Class Members' rights.

188. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff 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.

189. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large.

190. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid.

191. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

THIRD CAUSE OF ACTION
VIOLATION OF CALIFORNIA'S CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA")
(On behalf of the California Sub-Class)

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

193. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

194. Defendant is a "contractor" within the meaning of Civil Code § 56.05(d) within the meaning of Civil Code § 56.06 and/or a "business organized for the purpose of maintaining

medical information" and/or a "business that offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Defendant, within the meaning of Civil Code § 56.05(k).

195. Plaintiff and all members of the Class are "patients" within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiff and the Class fear that disclosure of their medical information could subject them to harassment or abuse.

196. Plaintiff and the respective Class members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network at the time of the breach.

197. Defendant, through inadequate security, allowed unauthorized third-party access to Plaintiff's and each Class member's medical information, without the prior written authorization of Plaintiff and the Class members, as required by Civil Code § 56.10 of the CMIA.

198. In violation of Civil Code § 56.10(a), Defendant disclosed Plaintiff's and the Class members' medical information without first obtaining an authorization. Plaintiff's and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.10(a).

199. In violation of Civil Code § 56.10(e), Defendant further disclosed Plaintiff's and the Class members' medical information to persons or entities not engaged in providing direct health care services to Plaintiff or the Class members or their providers of health care or health care service plans or insurers or self-insured employers.

200. Defendant violated Civil Code § 56.101 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the Class.

201. In violation of Civil Code § 56.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and the Class members' medical information in a manner that failed to preserve and breached the confidentiality of the information contained therein. Plaintiff's and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

202. In violation of Civil Code § 56.101(a), Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and the Class members' medical information. Plaintiff's and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

203. Plaintiff's and the Class members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

204. In violation of Civil Code § 56.101(b)(1)(A), Defendant's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. Plaintiff's and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(b)(1)(A).

205. Defendant violated Civil Code § 56.36 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the Class.

206. As a result of Defendant's above-described conduct, Plaintiff and the Class have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36.

207. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

208. Plaintiff, individually and for each member of the Class, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiff and each Class member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

FOURTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW
(On behalf of the California Sub-Class)

209. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

210. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

211. In the course of conducting its business, Defendant committed "unlawful" business practices by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and Class members' PII, and by violating the statutory and common law alleged herein. Plaintiff and Class members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

212. Defendant also violated the UCL's unlawful prong by obligations created by its Privacy Policy and by knowingly and willfully or, in the alternative, negligently and materially violating Cal. Bus. & Prof. Code § 22576, which prohibits a commercial website operator from "knowingly and willfully" or "negligently and materially" failing to comply with the provisions of their posted privacy policy. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Defendant's violations of their Privacy Policy.

213. Defendant also violated the UCL by failing to timely notify Plaintiff and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their Private Information. If Plaintiff and Class members had been notified in an appropriate

fashion, they could have taken precautions to safeguard and protect their Private Information and identities.

214. Defendant further violated the UCL by to use reasonable security measures under 45 C.F.R. § 164.530(c)(1), which 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."

215. Defendant also violated the UCL by failing 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.

216. Defendant also violated the UCL by violating New York's General Business Law § 349 by engaging in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services as more fully described above.

217. Defendant further violated the UCL by disseminating false and misleading statements in connection with its advertising in violation of Cal. Bus. & Prof. Code § 17500.

218. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the California

Consumer Privacy Act, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

219. Plaintiff and Class members suffered injury in fact and lost money or property as a result of Defendant's violations of its Privacy Policy and statutory and common law in that a portion of the money Plaintiff and Class members paid for Defendant's products and services went to fulfill the obligations set forth in their Privacy Policy, including maintaining the security of their PII, and Defendant's legal obligations and Defendant failed to fulfill those obligations.

220. The UCL also prohibits any "fraudulent business act or practice." Defendant's above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

221. Plaintiffs and members of the Class read and reasonably relied on Defendant's representations concerning its security practices and considered those representations material in deciding whether or not to transact with Defendant. Plaintiff and members of the Class similarly relied on Defendant to disclose any issues that contravened their express representations when deciding whether or not to transact with Defendant. Those misrepresentations and material omissions include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members Private Information, which was a proximate and direct 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. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

d. Failing to timely and adequately notify the Plaintiff and Class Members of the Data Breach;

e. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class Members' Private Information; and

g. 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 Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

222. Defendant's representations and 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 consumers' Private Information.

223. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers.

224. Defendant's representations and omissions were material because consumers understand the necessity of keeping such information secure and the consequences of identity theft.

225. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the UCL, Plaintiff and Class members have suffered injury in fact and lost money or property as a result of Defendant's unfair and deceptive conduct. Such injury includes paying for a certain level of security for their PII but receiving a lower level, paying more for Defendant's products and services than they otherwise would have had they known Defendant was not providing the reasonable security represented in their Privacy Policy and as in conformance with their legal obligations. Defendant's security practices have economic value in that reasonable security practices reduce the risk of theft of customer's PII.

226. Plaintiff and Class members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) deprivation of the value of their PII for which there is a well-established national and international market, and/or (iv) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

227. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of themselves, Class members, and the general public, also seeks equitable relief and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII

entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

FIFTH CAUSE OF ACTION
VIOLATION OF CONSUMER'S LEGAL REMEDIES ACT
Cal. Bus. & Prof. Code § 1750
(On behalf of the California Sub-Class)

228. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

229. Defendant's online prescription marketplace is a "service" as defined by California Civil Code §1761(a).

230. Defendant is a "person" as defined by California Civil Code §1761(c).

231. Plaintiff and Class members are "consumers" within the meaning of California Civil Code §1761(d) because they purchased Defendant's services for personal, family or household use.

232. The sale of Defendants' services to Plaintiff and Class members is a "transaction" as defined by California Civil Code §1761(e).

233. By misrepresenting the nature and sufficiency of Defendant's data and information security practices when Defendant knew or should have known that it's practices were insufficient and did not adequately protect consumer data, Defendant violated California Civil Code §§ 1770(a)(4), (5), (9) and (14), as it misrepresented the characteristics, benefits, rights, obligations, and remedies conferred by Defendant's prescription services. Prior to entering into an agreement to pay Defendants for its services, Plaintiff read and relied on the language in the Privacy Policy, including the language representing Defendant's privacy and security commitments, and agreed to pay money for Defendant's services.

234. As a result of Defendants' conduct, Plaintiff and Class members were harmed and suffered actual damages as a result of Defendant's unfair competition and deceptive acts and practices. Had Defendants disclosed the true nature and/or not falsely represented its Privacy Policy, Plaintiff and the Class would not have been misled into purchasing Defendant's services, or, alternatively, would have paid significantly less for them.

235. Plaintiff, on behalf of herself and all other similarly situated California consumers, and as appropriate, on behalf of the general public of the state of California, seeks injunctive relief prohibiting Defendants continuing these unlawful practices pursuant to California Civil Code § 1782(a)(2).

236. Plaintiff provided Defendants with notice of its alleged violations of the CLRA pursuant to California Civil Code § 1782(a) via certified mail, demanding that Defendant correct such violations.

237. If Defendant fails to respond to Plaintiff's CLRA letter within 30 days and fails to remedy the issues identified, Plaintiff will amend her complaint to seek all available damages under the CLRA for all violations complained of herein, including, but not limited to, statutory damages, punitive damages, attorney's fees and cost and any other relief that the Court deems proper.

SIXTH CAUSE OF ACTION
VIOLATION OF CALIFORNIA'S FALSE ADVERTISING LAW
Cal. Bus. & Prof. Code § 17500
(On behalf of the California Sub-Class)

238. At all material times, Defendants engaged in a scheme of offering their services for sale to Plaintiff, and other members of the Class by way of, inter alia, commercial marketing, and advertising, internet content, the Privacy Policy and other promotional materials.

239. These materials, advertisements, and other inducements misrepresented and/or omitted the true benefits of Defendant's security practices as alleged herein. Said materials, advertisements, and other inducements were controlled by and emanated from Defendant and were directed at consumers located in the State of California.

240. Defendants' advertisements and other inducements come within the definition of advertising as contained in Cal. Bus. Prof. Code § 17500, in that such promotional materials were intended as inducements to purchase Defendants' services and are statements disseminated by Defendants to Plaintiff and other members of the Class who are located in California.

241. A reasonable consumer would be misled by Defendants' Privacy Policy because Defendant represents the robustness of its commitment to data security and consumer privacy but Defendant did not and does not provide security sufficient to protect California consumer data from unauthorized access.

242. Plaintiff, a reasonable consumer, read and understood the language of the Privacy to mean that her data would be protected by reasonable, industry standard methods when in fact it was not, and in reliance thereon, agreed to pay for a Defendant's services.

SEVENTH COUNT
UNJUST ENRICHMENT
(On behalf of the National Class)

243. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

244. Plaintiff and Class Members conferred a benefit on Defendant with their money or labor services. Specifically, they purchased goods and services from Defendant and/or provided their labor and in so doing also provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the goods and services that

were the subject of the transaction and should have had their Private Information protected with adequate data security.

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

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

247. 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.

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

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

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

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

252. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

VII. PRAYER FOR RELIEF

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

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

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

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

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

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

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

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

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

VIII. JURY TRIAL DEMAND

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

DATED: June 27, 2022

Respectfully Submitted,

s/ Blake Hunter Yagman
Blake Hunter Yagman (SDNY No. 5644166)
byagman@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Tel.: (212) 594-5300

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

ATTORNEYS FOR PLAINTIFF

**Pro Hac Vice Forthcoming*