SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

MARGARET NEMETH, on behalf of herself and all others similarly situated, *Plaintiff*, v. NEW YORK-PRESBYTERIAN COLUMBIA UNIVERSITY IRVING MEDICAL CENTER and COLUMBIA UNIVERSITY HEALTH CARE, INC. *Defendants.*	Case No. _____ **SUMMONS**

New York county is designated as the place of trial. The basis of venue is that Defendant New York-Presbyterian Columbia University Irving Medical Center operates in New York County and a substantial part of the events, acts and omissions giving rise to Plaintiff's claims occurred in New York County. Defendant is a Manhattan based New York corporation located in New York County, New York at 630 West 168th Street, New York, New York.

TO THE ABOVE-NAMED DEFENDANT:

PLEASE TAKE NOTICE THAT YOU ARE SUMMONED to answer the complaint of the Plaintiff herein, and to serve a copy of your answer on the Plaintiff at the address indicated below within 20 days after service of this Summons (not counting the day of service itself), or within 30 days after service is complete if the Summons is not delivered personally to you within the State of New York.

YOU ARE HEREBY NOTIFIED THAT should you fail to answer, a judgment will be entered against you by default for the relief demanded herein.

DATED: October 22, 2024

Respectfully Submitted,

/s/ *Blake Hunter Yagman*

Blake Hunter Yagman
Edward Ciolko*
Jennifer Czeisler
STERLINGTON PLLC
One World Trade Center, 85th Floor
New York, New York 10007
Tel.: 929-709-1493
Email: *blake.yagman@sterlingtonlaw.com*
ed.ciolko@sterlingtonlaw.com
jen.czeisler@sterlingtonlaw.com

Attorneys for Plaintiff and the Proposed Class

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

MARGARET NEMETH, on behalf of herself and all others similarly situated, *Plaintiff*, v. NEW YORK-PRESBYTERIAN COLUMBIA UNIVERSITY IRVING MEDICAL CENTER and COLUMBIA UNIVERSITY HEALTH CARE, INC. *Defendants.*	Case No. _____ **SUMMONS**

New York county is designated as the place of trial. The basis of venue is that Defendant Columbia University Health Care, Inc. operates in New York County and a substantial part of the events, acts and omissions giving rise to Plaintiff's claims occurred in New York County. Defendant is a Manhattan based New York corporation located in New York County, New York whose registered agent is located at 110 Low Memorial Library, New York, New York, 10027.

TO THE ABOVE-NAMED DEFENDANT:

PLEASE TAKE NOTICE THAT YOU ARE SUMMONED to answer the complaint of the Plaintiff herein, and to serve a copy of your answer on the Plaintiff at the address indicated below within 20 days after service of this Summons (not counting the day of service itself), or within 30 days after service is complete if the Summons is not delivered personally to you within the State of New York.

YOU ARE HEREBY NOTIFIED THAT should you fail to answer, a judgment will be entered against you by default for the relief demanded herein.

DATED: October 22, 2024

Respectfully Submitted,

/s/ *Blake Hunter Yagman*

Blake Hunter Yagman
Edward Ciolko*
Jennifer Czeisler
STERLINGTON PLLC
One World Trade Center, 85th Floor
New York, New York 10007
Tel.: 929-709-1493
Email: *blake.yagman@sterlingtonlaw.com*
ed.ciolko@sterlingtonlaw.com
jen.czeisler@sterlingtonlaw.com

Attorneys for Plaintiff and the Proposed Class

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

MARGARET NEMETH, on behalf of herself and all others similarly situated,

Plaintiff,

v.

NEW YORK-PRESBYTERIAN COLUMBIA UNIVERSITY IRVING MEDICAL CENTER and COLUMBIA UNIVERSITY HEALTH CARE, INC.

Defendants.

Case No. _____

CLASS ACTION

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Margaret Nemeth ("Plaintiff"), on behalf of herself and all others similarly situated, alleges the following Class Action Complaint (the "Action") against the above-captioned Defendant, New York-Presbyterian Columbia University Irving Medical Center ("NYP") and Columbia University Health Care, Inc. ("CUIMC") (collectively, the "Defendants") 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. Columbia University Irving Medical Center "is a clinical, research and educational enterprise located [primarily] on a campus in northern Manhattan," New York City, New York as well as hospitals in Connecticut and New Jersey.[1] CUIMC "provides comprehensive patient care and offers a range of general and specialized medical, dental and nursing services."[2] With over 1,800 doctors and nurses in locations throughout the tri-state area, CUIMC is a sophisticated medical research and hospital center that aims to provide the "highest standard of care."[3]

2. In the course of serving New Yorkers, CUIMC collects a significant amount of data - including patients' personal identifiable information ("PII") first name and last name, date of birth, as well as protected health information including medical record numbers, provider name, and laboratory test results (the "PHI" or, collectively, the "PII"). This is the PII that was exposed for Plaintiff and the Class members.

[1] https://www.cuimc.columbia.edu/about-us/cuimc-facts-and-figures, (last accessed Oct. 15, 2024).

[2] *Id.*

[3] *Id.*

3. When patients initially disclosed this PII to Defendant, they did so under the impression that it would be protected in a manner consistent with how valuable this subset of PII is.

4. However, in May of 2024, Defendant disclosed that the PII of over 29,629 current or former patients, including the PII of Plaintiff and the putative Class, had been compromised in connection with a cyberattack that occurred between September 11, 2023 and March 7, 2024 (the "Data Breach").[4] This means that cybercriminals potentially had unfettered access to PII for nearly six months before CUIMC even detected any issues. This means that CUIMC's systems were insufficiently monitored for data breaches for almost half a year. To compound matters, CUIMC's response to the Data Breach was woefully sufficient: (1) CUIMC took over two months to notify individuals that their data was breached, this, in addition to the six months over which CUIMC's systems were invaded, means that for eight months Plaintiff and Class members had no knowledge that their PII was exposed; (2) CUIMC failed to explain how the Data Breach occurred and the measures being taken to prevent the same PII from falling into the hands of cybercriminals once again; (3) according to CUIMC, the Data Breach was the cause of an employee error in August 2023, but no notification of a potential breach was given then either to possible victims, and (4) CUIMC fails to offer any sort of compensation (including identity theft protection) for the harm caused by their inadequate cybersecurity protections.

5. Furthermore, the notice of the Data Breach (the "Notice") itself heavily underplays the seriousness of the Data Breach – which can further exacerbate harm to victims because victims will not take the proper precautions as a result of this Notice's failures. For example, the Notice states "[t]he type of breached information doesn't put the impacted persons in danger of identity

[4] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, (last accessed, Oct. 18, 2024).

theft," when the opposite is true.[5] CUIMC even acknowledges this in the next paragraph, as it warns against false claims made with insurers and payors as a result of the PII compromised in the Data Breach.

6. Due to this conduct, Plaintiff and Class members have been exposed to actual harm consistent with the litany of injuries that data breaches cause, including (a) loss of value of PII, (b) loss of time spent dealing with the Data Breach, (c) imminent threat of and actual theft of PII by cybercriminals, and (d) any other types of quantifiable harm that stem from the breach, including out-of-pocket losses and money spent on identity theft monitoring.

7. Notably, this is not CUIMC's first struggle to comply with basic cybersecurity principles resulting in consumer harm. In 2014, New York-Presbyterian and Columbia University paid the United States Department of Health and Human Services ("HHS") a $4.8 million settlement due to the unlawful sharing of patient information with Google.[6] The settlement, at the time, was the highest data breach settlement collected by HHS at the time.[7]

8. As such, Plaintiff, on behalf of herself and all other similarly situated, brings this Action to seek actual damages, punitive damages, restitution, statutory damages, injunctive relief, and a declaratory judgment, as well as any other relief this Court may deem just and proper, for CUIMC's negligence/negligence *per se*, breach of implied contract, violations of New York General Business Law 349, and unjust enrichment.

---

[5] https://www.defensorum.com/columbia-university-irving-medical-center-patient-data-exposed-online/, (last accessed, Oct. 15, 2024).

[6] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/new-york-and-presbyterian-hospital/index.html, (last accessed, Oct. 15, 2024).

[7] *Id.*

9. Additionally, given the scope of sensitive data compromised by CUIMC, offering no credit monitoring is insufficient to protect and remediate the harm caused by CUIMC's violations of law - Plaintiff and the putative Class seek at least three years of identity theft protection and credit monitoring.

II. JURISDICTION AND VENUE

10. *Personal Jurisdiction*. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in New York, New York. Furthermore, Defendant intentionally availed itself of this jurisdiction by marketing, employing individuals, and providing services in New York, New York.

11. *Venue*. Venue is proper in this Court pursuant to CPLR 503(a) because Defendant operates in this District and a substantial part of the events, acts and omissions giving rise to Plaintiff's claims occurred here, in this District.

III. PARTIES

Plaintiff Margaret Nemeth

12. Plaintiff Margaret Nemeth is a resident and citizen of the State of New Jersey and intends to remain domiciled in and a citizen of the State of New Jersey. Plaintiff received the Notice dated May 7, 2024. Plaintiff was informed that her sensitive PII was compromised in the Data Breach.

Defendant New York-Presbyterian Columbia University Irving Medical Center

13. Defendant NYP is a Manhattan-based, New York public benefit corporation located in New York County, New York at 630 West 168th Street, New York, New York. This address is also the address for CUIMC's privacy office, which can be found at box 159.[8]

[8] https://www.hipaa.cuimc.columbia.edu, (last accessed Oct. 15, 2024).

Defendant Columbia University Health Care, Inc.

14. Defendant CUIMC is a Manhattan-based, New York domestic, not for-profit corporation located in New York County. This entity can be served at Columbia University's Office of General Counsel, per the New York Department of State. Specifically, Columbia University Health Care, Inc.'s registered agent is located at 110 Low Memorial Library, New York, New York, 10027.[9]

IV. FACTUAL ALLEGATIONS

Defendant's Business

15. CUIMC is a major hospital system domiciled in Manhattan, New York, New York. Amongst the services that CUIMC offers are five hospitals spread throughout the tri-state area, including Helen Hayes Hospital of West Haverstraw, New York, Lawrence Hospital of Bronxville, New York, James J. Peters VA Medical Center of New York, Stamford Hospital of Stamford, Connecticut, and Valley Hospital of Ridgewood, New Jersey.[10] Each of these hospitals are maintained, owned, or operated by Defendant.

16. In the ordinary course of receiving health care services from CUIMC, patients are required to provide, at a minimum, the PII, which is the data set of information compromised in this Data Breach, as previously stated.

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

18. Additionally, with respect to medical care and protected health information, CUIMC may receive private and personal information from other individuals and/or organizations

[9] https://apps.dos.ny.gov/publicInquiry/EntityDisplay, (last accessed Oct. 15, 2024).

[10] https://www.cuimc.columbia.edu/about-us/cuimc-facts-and-figures, (last accessed Oct. 15, 2024).

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.

19. CUIMC also likely creates and maintains a considerable amount of PHI in the course of providing medical care and treatment. This PHI includes, but is not limited to, billing account numbers, financial information, medical record numbers, dates of service, provider names, and medical and clinical treatment information regarding care received from CUIMC.

20. According to CUIMC's Privacy Policy, CUIMC provides each of its patients with a HIPAA compliant notice of its privacy practices in respect to how they handle patients' sensitive and confidential information.

21. A copy of the Privacy Policy is maintained on CUIMC's website.

22. CUIMC 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 Policy without written authorization.

23. As a condition of receiving services and/or employment from Defendant, Defendant requires that its patients entrust it with highly sensitive personal information.

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

25. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

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

The Data Breach

27. On or about May 7, 2024, CUIMC notified victims of the Data Breach. This was done in part by disseminating a Data Breach notification letter as well as a notification on Defendant's website. The Data Breach notification letter received by Plaintiff reads in relevant part as follows:

> We are writing to let you know about a recent incident that may have involved certain personal information about you. We are taking this matter seriously and regret that it occurred.
>
> We were recently notified that a folder containing a file with personal information related to certain patients was inadvertently made available on a third-party internet accessible platform by a workforce member at [CUIMC]. The file was promptly secured and subsequently deleted from the platform, and an investigation was initiated.
>
> The workforce member inadvertently transferred the file containing patient lab data to that platform in or around August 2023 while performing certain quality-related data review activities. On March 8, 2024, we identified evidence that the folder containing the file may have been accessed or copied by unknown third parties between at least September 11, 2023 and March 7, 2024. The information contained in the file included: first name, last name, medical record number, date of birth, provider name, and a single laboratory test that would not reveal any diagnostic information about you…
>
> We are not aware of any misuse or further disclosure of your personal information in connection with this incident. As general good practice, it is recommended that you regularly monitor statements from your health plan for irregularities. If you notice any healthcare services that you did not receive listed on a statement, please contact your health plan.

28. The notice, which was signed and disseminated by Columbia University's Privacy Office, specifically by Chief Privacy Officer Karen Pagliaro-Meyer, related to this Data Breach raises significantly more questions than it answers.

29. *First,* CUIMC's largest failure is the fact that CUIMC did not detect that any information was at risk of exposure (or was actually exposed) until over half a year after unprotected, unencrypted patient data was first published online. This critical mistake means that CUIMC's network monitoring for intrusions was insufficient because unauthorized actors had access to patient data for a period of over half a year without detection. As a result, Plaintiff and Class members lost the ability to protect themselves until a significant time after their PII had been compromised. This evidences CUIMC's scant concern with the welfare for the people that they hold data for – because every moment after a data breach is precious and critical to a victim's ability to protect themselves and remediate harm.

30. *Next*, CUIMC fails to state when the investigation concluded, only that the download of this patient data took place between September 11, 2023 and March 7, 2024. While CUIMC detected that the data was downloaded by unauthorized third parties on March 8, 2024, at that point, it was far too late to protect this information from falling into the wrong hands.

31. *Finally,* CUIMC undermines the seriousness of the Data Breach before telling Plaintiff and Class members that, essentially, no compensation or identity theft monitoring would be available to victims and that victims would left to fed with the consequences of Defendant's actions and irresponsibility their own.

32. CUIMC's omissions within the Notice are also important: CUIMC fails to illuminate how the unauthorized actors initially gained access, why CUIMC failed to detect the intrusion(s) of these unauthorized actors, and specifically how CUIMC intends to avoid making these types of incidents from happening again. These critical points remain unclear.

33. 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.

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

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

36. On information and belief, the PII and PHI compromised in the files accessed by hackers was not encrypted – this can be presumed given the hackers were able to access the data that was stated as compromised in the Notice.

37. 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.

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

39. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of PII and PHI, the sophistication of Defendant, and the fact that Defendant is well aware of the risks of healthcare data breaches (as Defendant has an entire page on their website analyzing healthcare data breaches on a monthly basis), 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. This is highlighted by the fact that the Data Breach would not have occurred but for a CUIMC employee erroneously

uploading patient data onto an accessible server sans protection or encryption, as admitted by Defendant in the Notice.

40. This could have only occurred because 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 current and former patients' highly sensitive PHI; implementing guidelines for accessing, maintaining and communicating sensitive PHI, and protecting sensitive PHI by implementing protocols on how to utilize such information.

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

42. 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.

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

44. 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 Entirely Foreseeable

45. 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.

46. 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.

47. 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.

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

49. CUIMC'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 Data Breach.

50. Data breaches, including those perpetrated against the healthcare sector of the economy, have become widespread. Not surprisingly, healthcare is by far the most affected industry sector by data breaches and ransomware incidents. According to HIPAA statistics, between 2009 and 2022, 5,150 healthcare data breaches of 500 victims or more occurred. And, of those breaches, the impermissible disclosure of 382,262,109 healthcare records occurred. The rate of healthcare-related data breaches have also accelerated, with an average of approximately one large (500 victims or more) healthcare-related data breach per day in 2018 as compared to nearly two such data breaches per day in 2022. In 2023 alone, there were many large healthcare-related data breaches with tens of millions of victims including the MOVEit data breaches (tens of millions of victims across multiple data breaches), HCA Healthcare (11,270,000 victims), Perry Johnson & Associates (11,000,000+ victims), MCNA Dental (8,861,076 victims), and others. As such, CUIMC was aware of the risk of data breaches because such breaches have dominated the

headlines recently.

51. There is substantial evidence that data breaches in the healthcare sector harm patient outcomes. According to a 2019 Cornell University study titled "Do Hospital Data Breaches Reduce Patient Care Quality," "[h]ospital data breaches significant increase … mortality rate[.] Data breaches may disrupt the processes of care that rely on health information technology. Financial costs to repair a breach may also divert resources away from patient care. Thus, breached hospitals should carefully focus investments in security procedures, processes, and health information technology that jointly lead to better data security and improved patient outcomes."

52. 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."

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

54. 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."

55. 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."

56. 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.

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

58. 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.

59. 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.

60. 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.

61. 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

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

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

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

65. 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.

66. 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.

67. 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.

68. 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.

69. 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.").

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

71. 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.

72. 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

73. 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.

74. 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.

75. 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.

76. 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.

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

Defendant Failed to Comply with HIPAA

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

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

80. 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.

81. 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

82. 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).

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

Defendant's Breach

84. 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.

85. 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 and necessary 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).

86. 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.

87. 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

88. 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.

89. As previously stated, 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.

90. 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.

91. 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."

92. 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.

93. 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.

94. 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.

95. 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.

96. 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]

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

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

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

100. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose

of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

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

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

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

103. 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.

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

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

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

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

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

109. Medical information is especially valuable to identity thieves.

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

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

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

Harm to Plaintiff

113. On or about May 7, 2024, Plaintiff received notice from Defendant that her PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff's PII and PHI was compromised as a result of the Data Breach.

114. 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 by reviewing medical statements produced by her payors/insurers, valuable time Plaintiff otherwise would have spent on other activities.

115. Plaintiff suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her

PII, 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. Additionally, Plaintiff has realized an influx of spam emails and calls since the Data Breach occurred.

116. 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.

V. CLASS ALLEGATIONS

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

118. Plaintiff brings this Action on behalf of herself and all similarly situated persons for the following Class defined as:

> **Class Definition.** All individuals and entities residing in the United States whose PII and/or PHI was compromised on the Data Breach first announced by the Defendant in May of 2024.

(collectively, the "Class").

119. 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.

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

121. Numerosity. Defendant reports that the Data Breach compromised PHI of 29,000+ current and former patients. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

122. 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' PII;

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 PII;

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

g. Whether computer hackers obtained Class Members' PII 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.

123. 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 is 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.

124. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Class in that she 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.

125. 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.

126. The litigation of the claims brought herein is manageable. CUIMC'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.

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

128. 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.

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

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION

NEGLIGENCE

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

131. Defendant required Plaintiff and the Class Members to submit non-public personal information in order to obtain medical services.

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

133. 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.

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

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

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

137. 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.

138. 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.

139. 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 data breach incidents involving healthcare providers detailed above. Despite its knowledge of this foreseeable risk, Defendant failed to implement reasonable security measures.

140. 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.

141. 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.

142. 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.

143. Defendant's conduct also rises to the level of Negligence *per se*.

144. 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).

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

146. 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.

147. 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.

148. Defendant breached its duties, and thus was negligent (as well as negligent *per se*), by failing to use reasonable measures to protect the Class members' PHI and PII.

149. 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.

150. 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.

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

152. 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.

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

154. 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

BREACH OF IMPLIED CONTRACT

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

156. Defendant provides medical treatment and care to Plaintiff and Class members. Defendant formed an implied contract with Plaintiff and Class members through their collective conduct.

157. Through Defendant's provision of services, it knew or should have known that it must protect Plaintiff's and Class members' confidential PII and PHI in accordance with Defendant's stated policies, practices and applicable law.

158. As consideration, Plaintiff and Class members turned over valuable PII and PHI in exchange for either medical services or care.

159. Defendant accepted possession of Plaintiff's and Class members' PII and PHI for the purpose of providing services to Plaintiff and the Class members. In delivering their PII and PHI to Defendant, Plaintiff and the Class members intended and understood that Defendant would adequately safeguard the PII as part of the provision or receipt of those services.

160. Defendant's implied promises to Plaintiff and Class members include, but are not limited to Defendant: (1) taking steps to ensure that anyone who is granted access to PII and PHI also protects the confidentiality of that data; (2) taking steps to ensure that the PII and PHI placed in control of Defendant's employees is restricted and limited only to achieve authorized business purposes; (3) restricting access to employees and/or agents who are qualified and trained; (4) designing and implementing appropriate retention policies to protect PII and PHI; (5) applying or requiring proper encryption and/or the separation of different data sets; (6) implementing multifactor authentication for access; and (7) taking other steps to protected against foreseeable breaches.

161. Plaintiff and Class members would not have entrusted their PII and PHI to Defendant in the absence of such an implied contract.

162. Defendant violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class members' PII and PHI.

163. Plaintiff and Class members have been damaged by Defendant's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein. Plaintiff seeks damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION

VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349

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

165. Plaintiff and the Class Members are consumers as defined by the statute because they received services from a New York-based Defendant, their data was collected by a New York-based Defendant, and the harm caused to them was due to the poor decision-making and negligent conduct of a New York-based Defendant.

166. 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 PII and PHI, 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' PHI and PII, 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. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class Members' PII and PHI; and

f. 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' PII and PHI, 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.

167. 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 PII and PHI.

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

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

170. 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 PII and PHI.

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

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

173. Plaintiff and Class Members paid a price higher for medical services that they ordinarily would not have due to the cost of Defendant's ineffective cybersecurity apparatus and protocols. This premium pricing was not justified, as the Data Breach reveals.

174. 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.

FOURTH CAUSE OF ACTION

UNJUST ENRICHMENT

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

176. This Count is alternatively pled to Count III, Breach of Implied Contract.

177. 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 PII and PHI. 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 PII and PHI protected with adequate data security.

178. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII and PHI of Plaintiff and Class Members for business purposes.

179. In particular, the Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' PII and PHI. 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.

180. 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.

181. Defendant failed to secure Plaintiff's and Class Members' PII and PHI and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

182. Defendant acquired the PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

183. If Plaintiff and Class Members knew that Defendant had not reasonably secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

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

185. 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 PII and PHI is used; (c) the compromise, publication, and/or theft of their PII and PHI; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (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 PII and PHI, 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 PII and PHI 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 PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

186. 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.

187. 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

188. 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 her 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

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

DATED: October 22, 2024

Respectfully Submitted,

/s/ *Blake Hunter Yagman*

Blake Hunter Yagman
Edward Ciolko*
Jennifer Czeisler
STERLINGTON PLLC
One World Trade Center, 85th Floor
New York, New York 10007
Tel.: 929-709-1493
Email: *blake.yagman@sterlingtonlaw.com*
ed.ciolko@sterlingtonlaw.com
jen.czeisler@sterlingtonlaw.com

Attorneys for Plaintiff and the Proposed Class