SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF SCHENECTADY

----------X

JEANETTE CONIGLIO, on behalf of herself and all others similarly situated,

Plaintiff,

-against-

CARENET MEDICAL GROUP, PC,

Defendant.

----------X

INDEX NO: _____
Plaintiff designates Schenectady County as the place of Trial.

SUMMONS

The basis of venue is Defendant's principal office, located at 2123 River Road, Schenectady, New York 12309

To the above named defendant:

YOU ARE HEREBY SUMMONED and required to serve upon Plaintiffs' attorneys an answer to the complaint in this action within twenty days after the service of this summons, exclusive of the day of service, or within thirty days after service is complete if this summons is not personally delivered to you within the State of New York. In case of your failure to answer, judgment will be taken against you by default for the relief demanded in the complaint.

__/s/ James J. Bilsborrow_____
James J. Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, New York 10003
(212) 558-5500

Cassandra P. Miller*
cmiller@straussborrelli.com
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
**Pro Hac Vice forthcoming*

Counsel for Plaintiffs and the Proposed Class

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF SCHENECTADY

----------X

JEANETTE CONIGLIO, on behalf of herself and all others similarly situated,

Plaintiff,

-against-

CARENET MEDICAL GROUP, PC,

Index No.
JURY DEMAND

Defendant.

----------X

CLASS ACTION COMPLAINT

Jeanette Coniglio ("Plaintiff"), through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant CareNet Medical Group, PC ("CareNet" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to her own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant is a medical provider of obstetric and gynecologic services.[1]

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about its

[1] *Home*, CARENET MEDICAL GROUP, https://www.carenetmedical.com/ (last accessed Oct. 19, 2023).

current and former patients. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach")

4. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former patients' PII/PHI.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI. In short, Defendant's failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim. She brings this class action on behalf of herself, and all others harmed by Defendant's misconduct.

7. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, patients' private information was exactly that—private. Not anymore. Now, patients' private information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Jeanette Coniglio, is natural person and adult citizen of Greenville, New York. Ms. Coniglio intends to remain domiciled in New York indefinitely, and maintains her true, fixed, and permanent home in Bath, New York.

9. Defendant, CareNet Medical Group, PC, is a domestic professional service corporation incorporated in New York with its principal place of business at 2123 River Road, Schenectady, New York 12309.

JURISDICTION AND VENUE

10. Defendant regularly and systematically conducts business and provides medical services in this county, and sells products and services to its customers, including Plaintiffs and members of the putative class, in this county. As such, it is subject to the jurisdiction of this Court.

11. This Court has personal jurisdiction over Defendant because it is incorporated in New York and its corporate headquarters are in this County.

12. Venue is proper in this Court because a substantial part of the alleged wrongful conduct and events giving rise to the claims occurred in this County and because Defendant conducts significant business in this County.

BACKGROUND

Defendant Collected and Stored the PII/PHI of Plaintiff and the Class

13. Defendant is a medical provider of obstetric and gynecologic services.[2]

14. As part of its business, Defendant receives and maintains the highly sensitive PII/PHI of thousands of its current and former patients. In fact, Defendant admits that:

a. "Protected Health Information (PHI), about you, is maintained as a written and/or electronic record of your contacts or visits for healthcare services with our practice."[3]

b. "Specifically, PHI is information about you, including demographic information, (i.e., name, address, telephone number, etc…), that may

[2] *Home,* CARENET MEDICAL GROUP, https://www.carenetmedical.com/ (last accessed Oct. 19, 2023).
[3] *Notice of Privacy Practices (HIPAA)*, CARENET (Aug. 1, 2013) https://static1.squarespace.com/static/635d8d3ab5d4b729bd43cbcb/t/63a7085073fa20232a0ee871/1671891024318/npp.pdf.

identify you and relates to your past, present or future physical or mental health condition and related healthcare services."[4]

15. In collecting and maintaining the PII/PHI, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PII/PHI.

16. Under state and federal law, businesses like Defendant have duties to protect its current and former patients' PII/PHI and to notify them about breaches.

17. Defendant recognizes these duties. For example, in its "Notice of Privacy Practices (HIPPA)," Defendant declares that:

a. "Our practice is dedicated to maintaining the privacy of your individually identifiable health information."[5]

b. "By federal and state law, we must follow the terms of the notice of privacy practices that we have in effect at the time."[6]

c. "Our practice is required to follow specific rules on maintaining the confidentiality of your PHI, using your information, and disclosing or sharing this information."[7]

d. "Uses and disclosures of your protected health information that involve the release of psychotherapy notes (if any), marketing, sale of your protected health information, or other uses and disclosures not described in this notice

[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*

or required by law will be made only with your separate written permission."[8]

18. Moreover, Defendant explains that "we may use and disclose protected health information about you" only in eight specific permissible situations—none of which include the unauthorized exposure to cybercriminals in a data breach.[9]

19. And in its "Privacy Policy," Defendant declares that:

a. "We are committed to the right to privacy for our patients."[10]

b. "It is our policy not to share the information with third parties for any reason, unless legally required to do so or as necessary to process your requests."[11]

Defendant's Data Breach

20. From May 9, 2022, to June 4, 2022, Defendant was hacked by cybercriminals.[12]

21. And Defendant admits that the cybercriminals were successful—having "removed certain files and folders from portions of its network which contained protected health information."[13]

22. Because of Defendant's Data Breach, at least the following types of PII/PHI were compromised:

a. full names,

[8] *Id.*
[9] *Id.*
[10] *Privacy Policy*, CARENET, https://www.carenetmedical.com/privacy (last accessed Oct. 19, 2023).
[11] *Id.*
[12] *Data Breach*, CARENET, https://www.carenetmedical.com/data-breach (last accessed Oct. 19, 2023).
[13] *Id.*

b. addresses,

c. driver's license numbers,

d. bank account numbers,

e. bank account routing numbers,

f. dates of birth,

g. medical reference numbers,

h. Medicare numbers,

i. cell phone numbers,

j. home phone numbers,

k. health insurance information,

l. email addresses, and

m. Social Security Numbers.[14]

23. In total, Defendant injured at least 10,059 persons—via the exposure of their PII/PHI—in the Data Breach.[15] Upon information and belief, these 10,059 persons include Defendant's current and former patients.

24. Stunningly, Defendant waited until June 2, 2023, before it began notifying the class—a full *389 days after* the Data Breach began.[16]

25. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

[14] *Id*.
[15] *Breach Report*, US DEPT HEALTH HUMAN SERVS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Oct. 19, 2023).
[16] *Data Breach*, CARENET, https://www.carenetmedical.com/data-breach (last accessed Oct. 19, 2023).

26. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class:

a. "If you are very concerned about becoming a victim of fraud or identity theft, you may request a 'Security Freeze' be placed on your credit file."[17]

b. "[P]lace a security freeze on your credit report by contacting all three nationwide credit reporting companies."[18]

c. "Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company."[19]

d. "Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or care provider for any items you do not recognize."[20]

e. "[O]btain information about preventing identity theft from the New York Attorney General's Office."[21]

f. "[C]all your local law enforcement agency and file a police report."[22]

27. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data

[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*

Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused widespread injury and monetary damages.

28. Since the breach, Defendant has "taken additional precautions to safeguard [PII/PHI]."[23] But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

29. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

30. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring. But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class members for the injuries that Defendant inflicted upon them.

31. Because of Defendant's Data Breach, the sensitive PII/PHI of Plaintiff and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class members.

32. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) gained actual access to sensitive data, and (3) successfully "removed certain files and folders."[24]

33. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the dark web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[25]

---

[23] *Id*.
[24] *Id*.
[25] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

34. Thus, on information and belief, Plaintiff's and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

Plaintiff's Experiences and Injuries

35. Plaintiff was a patient of Defendant from approximately 2014 until 2022.

36. Thus, Defendant obtained and maintained Plaintiff's PII/PHI.

37. As a result, Plaintiff Jeanette Coniglio was injured by Defendant's Data Breach.

38. Plaintiff provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

39. Plaintiff reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII/PHI.

40. Plaintiff does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

41. Thus, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

42. Plaintiff called the toll-free response line established by Defendant. The response line then took down Plaintiff's information and promised her that they would call her back the next day. But the response line failed to do so.

43. Upon information and belief, through its Data Breach, Defendant compromised Plaintiff's:

a. full name,

b. address,

c. driver's license number,

d. bank account number,

e. bank account routing number,

f. date of birth,

g. medical reference number,

h. Medicare number,

i. cell phone number,

j. home phone number,

k. health insurance information,

l. email address, and

m. Social Security Number.

44. Worryingly, in the aftermath of the Data Breach, Plaintiff *already* suffered from multiple instances of identity theft and fraudulent charges on her Pioneer Bank debit card:

a. $35.89 for Lyft on May 6, 2022;

b. $201.04 for Lyft on May 6, 2022;

c. $18.84 for Lyft on May 9, 2022;

d. $52.33 for Uber on July 13, 2022; and

e. $93.19 for Uber on July 13, 2022.

45. Tellingly, these fraudulent charges were on the very debit card that Plaintiff used at Defendant's office.

46. Specifically, Plaintiff suffered from these instances of identity theft and fraud from approximately May 2022 to August 2022. Thus, Plaintiff's injuries precisely coincide with the dates of the Data Breach (May 2022 to June 2022).

47. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

48. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

49. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

50. Plaintiff suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

51. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

52. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.

53. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

54. Today, Plaintiff has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

55. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII/PHI.

56. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to $1,000.00 depending on the type of information obtained.

57. The value of Plaintiff and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

58. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

59. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

60. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

61. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

62. Defendant disclosed the PII/PHI of Plaintiff and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI of Plaintiff and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

63. Defendant's failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff and Class members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

64. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

65. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[26] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[27] Those 330 reported breaches exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[28]

66. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings 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."[29]

67. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare

---

[26] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.
[27] *Id.*
[28] *Id.*
[29] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

organizations experienced cyberattacks in the past year.[30]

68. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

69. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

70. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[31] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

71. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

72. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

---

[30] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Sept. 11, 2023).

[31] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

73. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use 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.

74. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

75. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: 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.

76. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers;

monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

77. 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.

78. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Defendant Violated HIPAA

79. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[32]

80. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI and PHI is properly maintained.[33]

[32] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[33] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

81. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any 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);

d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. 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);

f. 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);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security

incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

82. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

83. Plaintiff brings action pursuant to Civil Practice Law and Rules (CPLR) Article 9 on behalf of herself and all members of the proposed class (the "Class"), defined as follows:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach experienced by CareNet in or around May 2022 to June 2022 including all those who received notice of the breach.

84. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

85. Plaintiff reserves the right to amend the class definition.

86. This action satisfies the numerosity, predominance, typicality, adequacy, and superiority requirements under New York CPLR § 901.

87. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

88. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least 10,059 members.

89. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII/PHI;

b. if 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. if Defendant were negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII/PHI;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

90. Typicality. Plaintiff's claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

91. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. her interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

92. Superiority. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

93. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

94. Plaintiff and the Class entrusted their PII/PHI to Defendant on the premise and with the understanding that Defendant would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

95. Defendant owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

96. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

97. Defendant owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class members' PII/PHI.

98. Defendant owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their PII/PHI.

99. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required

and necessary for Plaintiff and Class members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

100. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

101. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

102. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

103. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff and Class members' PII/PHI.

104. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class members' sensitive PII/PHI.

105. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and

amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

106. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class members' PHI.

107. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

108. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendant hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII/PHI —whether by malware or otherwise.

109. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff and Class members' and the importance of exercising reasonable care in handling it.

110. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

111. Defendant breached these duties as evidenced by the Data Breach.

112. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' PII/PHI by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

113. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII/PHI of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

114. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class members' injuries-in-fact.

115. Defendant has admitted that the PII/PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

116. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

117. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

118. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class members actual,

tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

119. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

120. Plaintiff and Class members were required to provide their PII/PHI to Defendant as a condition of receiving medical services provided by Defendant. Plaintiff and Class members provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's medical services.

121. Plaintiff and Class members reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

122. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

123. Plaintiff and the Class members accepted Defendant's offers by disclosing their PII/PHI to Defendant or its third-party agents in exchange for medical services.

124. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

125. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII/PHI.

126. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class members with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

127. After all, Plaintiff and Class members would not have entrusted their PII/PHI to Defendant or its third-party agents in the absence of such an agreement with Defendant.

128. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

129. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

130. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

131. Defendant materially breached the contracts it entered with Plaintiff and Class members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

132. In these and other ways, Defendant violated its duty of good faith and fair dealing.

133. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed *supra*).

134. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

135. Plaintiff and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

136. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

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

138. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII/PHI to provide medical services and facilitate collection of payment.

139. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members. And Defendant benefited from receiving Plaintiff's and Class members' PII/PHI, as this was used to provide medical services and facilitate collection of payment.

140. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

141. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII/PHI.

142. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of 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 failure to provide the requisite security.

143. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' PII/PHI and/or payment because Defendant failed to adequately protect their PII/PHI.

144. Plaintiff and Class members have no adequate remedy at law.

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

FOURTH CAUSE OF ACTION
Violation of N.Y. Gen. Bus. Law § 349 *et seq*.
(On Behalf of Plaintiff and the Class)

146. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

147. New York General Business Law § 349 ("GBL § 349") prohibits deceptive acts or practices in the conduct of any business, trade, or commerce or in the furnishing of any service in the state of New York.

148. GBL § 349 applies to Defendant because Defendant engages in business, trade, or commerce in New York. And Defendant's acts and practices were directed at Plaintiff and the Class.

149. Defendant violated GBL § 349 by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII/PHI, which was a direct and proximate cause of the Data Breach;

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

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

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII/PHI; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII/PHI, including duties

imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

150. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their PII/PHI.

151. Defendant intended to mislead Plaintiff and Class members and induce them to rely on its omissions.

152. Had Defendant disclosed to Plaintiff and Class members that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII/PHI that Plaintiff and Class members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

153. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class members' rights.

154. As a direct and proximate result of Defendant's unfair and deceptive 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/PHI.

155. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the dark web.

156. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law.

FIFTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

157. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

158. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

159. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

160. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

161. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

162. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

163. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class members' injuries.

164. If an injunction is not issued, the resulting hardship to Plaintiff and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

165. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class members, and the public at large.

PRAYER FOR RELIEF

Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: June 28, 2024

WEITZ & LUXENBERG, PC

By: /s/ James J. Bilsborrow

James Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
Telephone: (212) 558-5500
jbilsborrow@weitzlux.com

Cassandra P. Miller*
cmiller@straussborrelli.com
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109

**Pro Hac Vice forthcoming*

Counsel for Plaintiffs and the Proposed Class