ANDREW W. FERICH
aferich@ahdootwolfson.com
NJ Bar ID No. 015052012
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Tel: (310) 474-9111
Fax: (310) 474-8585

BRADLEY K. KING
bking@ahdootwolfson.com
NJ Bar ID No. 081472013
AHDOOT & WOLFSON, PC
521 Fifth Avenue, 17th Floor
New York, NY 10175
Tel: (917) 336-0171
Fax: (917) 336-0177

[Additional class counsel appear on signature page]

Interim Class Counsel

ELIO LEPORE, RONALD SIGNORINO, DAVID BERMAN, RICHARD WEISS, CHARLES ZISS, and MARYANN JOYCE, individually and on behalf of all others similarly situated, Plaintiffs, v. AFFILIATED DERMATOLOGISTS & DERMATOLOGIC SURGEONS, P.A., Defendant.	SUPERIOR COURT OF NEW JERSEY LAW DIVISION: MORRIS COUNTY Case No. MRS-L-001091-24 **CONSOLIDATED CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Elio Lepore, Ronald Signorino, David Berman, Richard Weiss, Charles Ziss, and MaryAnn Joyce, individually and on behalf of all others similarly situated (collectively, "Class Members"), by and through their attorneys, bring this Consolidated Class Action Complaint against Defendant Affiliated Dermatologists & Dermatologic Surgeons, P.A. ("Defendant") and

allege upon personal knowledge as to their own actions and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to secure and safeguard their and approximately 373,379 other individuals' private and confidential medical information, including names, dates of birth, Social Security numbers ("SSN"), medical treatment information, health insurance claims information, driver's license numbers, and passport numbers ("PII/PHI").

2. Defendant is a private dermatology, surgery, laser, and cosmetic dermatology practice located in Morristown, New Jersey.

3. On or about March 5, 2024, Defendant discovered that "an unauthorized third party gained access and left a ransom note on Defendant's network."[1] Defendant's investigation revealed that, between March 2, 2024, and March 5, 2024, the unauthorized actor obtained access or acquired certain files stored on Defendant's network, including Plaintiffs' and Class Members' PII/PHI ("Data Breach"). Defendant did not begin notifying consumers of this Data Breach until May 23, 2024.[2] Defendant completed its investigation of the Data Breach on April 10, 2024.[3]

4. Defendant owed a duty to Plaintiffs and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendant breached that duty by, among other things, failing

[1] *Notice of Data Security Incident*, AFFILIATEDDERMATOLOGISTS.COM, https://www.affiliateddermatologists.com/storage/app/media/24-05-20-updated-draft-substitute-notice-affiliated-dermatologist2971080371-1.pdf (last accessed Sept. 27, 2024) ("Notice Letter").
[2] *Id.*
[3] *Id. at* 1.

to implement and maintain reasonable security procedures and practices to protect its patients' and employees' PII/PHI from unauthorized access and disclosure.

5. Defendant also owed a duty to notify Plaintiffs and Class Members as soon as reasonably possible about the Data Breach, but it breached that duty by waiting nearly two months after the Data Breach was discovered to send out the Notice Letter.

6. Defendant failed to implement adequate cybersecurity measures, despite possessing the financial resources and technological means to do so. Its misconduct includes failing to detect and prevent the Data Breach, failing to encrypt sensitive data, failing to adequately notify affected individuals in a timely manner, and not taking necessary steps to safeguard data post-breach.

7. Defendant also breached its obligations under federal laws, such as Section 5 of the Federal Trade Commission Act ("FTC Act"), the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), and 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules"), by failing to implement reasonable security practices, failing to comply with industry-standard data protection measures, and failing to provide timely notice of the Data Breach.

8. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class Members' PII/PHI was accessed and disclosed. This action seeks to remedy Defendant's failures and its consequences. Plaintiffs bring this action on behalf of themselves and all United States residents whose PII/PHI was compromised in the Data Breach.

9. The Data Breach exposed Plaintiffs and Class Members to significant risks, including identity theft, fraud, misappropriation of health insurance benefits, and other criminal activity. Plaintiffs and Class Members now face the burdens of monitoring credit, financial accounts, health records, and personal communications, as well as taking preventative measures, all of which require substantial time and money.

10. Plaintiffs also experienced diminished control over their PII/PHI and continue to be exposed to heightened risks of identity theft. Some Plaintiffs have already suffered tangible harms, such as financial loss, loss of privacy, and increased spam communications.

11. Plaintiffs seek a range of remedies to address both past and future harms, including compensation for financial losses, identity theft prevention services, enhanced data security protocols, and periodic audits to ensure compliance with cybersecurity standards.

12. Plaintiffs, individually and on behalf of all other Class Members, assert claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, invasion of privacy, violation of the New Jersey Consumer Fraud Act, and unjust enrichment, and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Elio Lepore

13. Plaintiff Elio Lepore is a resident and citizen of East Hanover, New Jersey. Plaintiff Lepore's PII/PHI was provided to or obtained by Defendant in connection with its provision of medical treatment and services. Believing Defendant would implement and maintain reasonable security practices to protect his PII/PHI, Plaintiff Lepore routinely provided his PII/PHI to Defendant in connection with receiving medical treatment and services.

14. Plaintiff Lepore is careful about sharing his PII/PHI and takes reasonable steps to protect his PII/PHI. Plaintiff Lepore has never knowingly transmitted unencrypted PII/PHI over the internet or other unsecured source. Plaintiff Lepore stores any documents containing PII/PHI in a safe and secure location and diligently chooses unique usernames and passwords for his online accounts.

15. At the time of the Data Breach, Defendant retained Plaintiff Lepore's PII/PHI in its systems, and on information and belief, it continues to retain that information.

16. Plaintiff Lepore first learned of the Data Breach after receiving a Notice Letter from Defendant dated May 23, 2024, notifying him of the Data Breach and that his PII/PHI had been improperly accessed and disclosed to unauthorized third parties. This Notice Letter confirmed that his name, date of birth, mailing address, SSN, medical treatment information, and health insurance claims information may have been included in the compromised database.

17. Upon receiving notice of the Data Breach, Plaintiff Lepore made reasonable efforts to mitigate its impact, including, but not limited to, verifying the legitimacy of the Notice of Data Breach, monitoring his various financial and banking accounts for fraudulent activity, and freezing his credit with Experian, TransUnion, and Equifax.

18. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Lepore will need to maintain these heightened measures for years.

19. In the time following the Data Breach, Plaintiff Lepore has experienced an increase in spam emails and phone calls. Additionally, on or about August 23, 2024, Plaintiff Lepore received a phone alert form his bank notifying him that his SSN was found on the dark web.

20. Plaintiff Lepore also suffered actual injury from having his PII/PHI compromised

as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential PII/PHI—a form of property that was entrusted to Defendant and was compromised as a result of the Data Breach Defendant failed to prevent, and (b) a violation of Plaintiff's privacy rights as a result of unauthorized disclosure of his PII/PHI.

21. Plaintiff Lepore has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because Defendant disclosed his PII/PHI to unauthorized parties who may now use that information for improper and unlawful purposes.

22. Plaintiff Lepore is exposed, and will continue to be exposed for the remainder of his life, to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his PII/PHI being obtained by unauthorized third parties and/or cybercriminals.

23. Plaintiff Lepore is also at a continued risk of harm because, on information and belief, his PII/PHI remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the PII/PHI in its possession.

24. Plaintiff Lepore has a continuing interest in ensuring that his PII/PHI, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks.

Plaintiff Ronald Signorino

25. Plaintiff Ronald Signorino is a resident and citizen of Basking Ridge, New Jersey. Plaintiff Signorino's PII/PHI was provided to or obtained by Defendant in connection with its provision of medical treatment and services. Believing Defendant would implement and maintain

reasonable security practices to protect his PII/PHI, Plaintiff Signorino routinely provided his PII/PHI to Defendant in connection with receiving medical treatment and services.

26. Plaintiff Signorino is careful about sharing his PII/PHI and takes reasonable steps to protect his PII/PHI. Plaintiff Signorino has never knowingly transmitted unencrypted PII/PHI over the internet or other unsecured source. Plaintiff Signorino stores any documents containing PII/PHI in a safe and secure location and diligently chooses unique usernames and passwords for his online accounts.

27. At the time of the Data Breach, Defendant retained Plaintiff Signorino's PII/PHI in its systems, and on information and belief, it continues to retain that information.

28. Plaintiff Signorino first learned of the Data Breach after receiving a Notice Letter from Defendant dated May 23, 2024, notifying him of the Data Breach and that his PII/PHI had been improperly accessed and disclosed to unauthorized third parties. This Notice Letter confirmed that his name, date of birth, mailing address, SSN, medical treatment information, and health insurance claims information may have been included in the compromised database.

29. Upon receiving notice of the Data Breach, Plaintiff Signorino made reasonable efforts to mitigate its impact, including, but not limited to, signing up for credit monitoring, contacting credit card issuers and financial institutions and changing passwords.

30. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Signorino will need to maintain these heightened measures for years.

31. In the time following the Data Breach, Plaintiff Signorino has experienced an increase in spam emails and phone calls.

32. Plaintiff Signorino also suffered actual injury from having his PII/PHI

compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential PII/PHI—a form of property that was entrusted to Defendant and was compromised as a result of the Data Breach Defendant failed to prevent, and (b) a violation of Plaintiff's privacy rights as a result of unauthorized disclosure of his PII/PHI.

33. Plaintiff Signorino has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because Defendant disclosed his PII/PHI to unauthorized parties who may now use that information for improper and unlawful purposes.

34. Plaintiff Signorino is exposed, and will continue to be exposed for the remainder of his life, to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his PII/PHI being obtained by unauthorized third parties and/or cybercriminals.

35. Plaintiff Signorino is also at a continued risk of harm because, on information and belief, his PII/PHI remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the PII/PHI in its possession.

36. Plaintiff Signorino has a continuing interest in ensuring that his PII/PHI, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks.

Plaintiff David Berman

37. Plaintiff David Berman is a resident and citizen of Morristown, New Jersey. Plaintiff Berman's PII/PHI was provided to or obtained by Defendant in connection with its provision of medical treatment and services. Believing Defendant would implement and maintain

reasonable security practices to protect his PII/PHI, Plaintiff Berman routinely provided his PII/PHI to Defendant in connection with receiving medical treatment and services.

38. Plaintiff Berman is careful about sharing his PII/PHI and takes reasonable steps to protect his PII/PHI. Plaintiff Berman has never knowingly transmitted unencrypted PII/PHI over the internet or other unsecured source. Plaintiff Berman stores any documents containing PII/PHI in a safe and secure location and diligently chooses unique usernames and passwords for his online accounts.

39. At the time of the Data Breach, Defendant retained Plaintiff Berman's PII/PHI in its systems, and on information and belief, it continues to retain that information.

40. Plaintiff Berman first learned of the Data Breach after receiving a Notice Letter from Defendant dated May 23, 2024, notifying him of the Data Breach and that his PII/PHI had been improperly accessed and disclosed to unauthorized third parties. This Notice Letter confirmed that his name, date of birth, mailing address, SSN, medical treatment information, and health insurance claims information may have been included in the compromised database.

41. Upon receiving notice of the Data Breach, Plaintiff Berman made reasonable efforts to mitigate its impact, including, but not limited to, spending approximately two hours to date calling Defendant to receive more information about the Data Breach and the credit monitoring company listed in the Notice Letter.

42. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Berman will need to maintain heightened mitigation measures for years.

43. In the time following the Data Breach, Plaintiff Berman has experienced an increase in phishing and spam emails.

44. Plaintiff Berman also suffered actual injury from having his PII/PHI compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential PII/PHI—a form of property that was entrusted to Defendant and was compromised as a result of the Data Breach Defendant failed to prevent, and (b) a violation of Plaintiff's privacy rights as a result of unauthorized disclosure of his PII/PHI.

45. Plaintiff Berman has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because Defendant disclosed his PII/PHI to unauthorized parties who may now use that information for improper and unlawful purposes.

46. Plaintiff Berman is exposed, and will continue to be exposed for the remainder of his life, to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his PII/PHI being obtained by unauthorized third parties and/or cybercriminals.

47. Plaintiff Berman is also at a continued risk of harm because, on information and belief, his PII/PHI remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the PII/PHI in its possession.

48. Plaintiff Berman has a continuing interest in ensuring that his PII/PHI, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks.

Plaintiff Richard Weiss

49. Plaintiff Richard Weiss is a resident and citizen of Westchester County, New Jersey. Plaintiff Weiss' PII/PHI was provided to or obtained by Defendant in connection with its provision

of medical treatment and services. Believing Defendant would implement and maintain reasonable security practices to protect his PII/PHI, Plaintiff Weiss routinely provided his PII/PHI to Defendant in connection with receiving medical treatment and services.

50. Plaintiff Weiss is careful about sharing his PII/PHI and takes reasonable steps to protect his PII/PHI. Plaintiff Weiss has never knowingly transmitted unencrypted PII/PHI over the internet or other unsecured source. Plaintiff Weiss stores any documents containing PII/PHI in a safe and secure location and diligently chooses unique usernames and passwords for his online accounts.

51. At the time of the Data Breach, Defendant retained Plaintiff Weiss' PII/PHI in its systems, and on information and belief, it continues to retain that information.

52. Plaintiff Weiss first learned of the Data Breach after receiving a Notice Letter from Defendant dated May 23, 2024, notifying him of the Data Breach and that his PII/PHI had been improperly accessed and disclosed to unauthorized third parties. This Notice Letter confirmed that his name, date of birth, mailing address, SSN, medical treatment information, and health insurance claims information may have been included in the compromised database.

53. Upon receiving notice of the Data Breach, Plaintiff Weiss made reasonable efforts to mitigate its impact, including, but not limited to, researching the Data Breach, placing a freeze on his credit reports, thoroughly reviewing his account statements and financial transactions, screening spam calls, and taking other steps in an attempt to protect himself following the Data Breach.

54. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Weiss will need to maintain these heightened measures for years.

55. In the time following the Data Breach, Plaintiff Weiss has experienced an increase in spam emails and phone calls.

56. Plaintiff Weiss also suffered actual injury from having his PII/PHI compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential PII/PHI—a form of property that was entrusted to Defendant and was compromised as a result of the Data Breach Defendant failed to prevent, and (b) a violation of Plaintiff's privacy rights as a result of unauthorized disclosure of his PII/PHI.

57. Plaintiff Weiss has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because Defendant disclosed his PII/PHI to unauthorized parties who may now use that information for improper and unlawful purposes.

58. Plaintiff Weiss is exposed, and will continue to be exposed for the remainder of his life, to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his PII/PHI being obtained by unauthorized third parties and/or cybercriminals.

59. Plaintiff Weiss is also at a continued risk of harm because, on information and belief, his PII/PHI remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the PII/PHI in its possession.

60. Plaintiff Weiss has a continuing interest in ensuring that his PII/PHI, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks.

Plaintiff Charles Ziss

61. Plaintiff Charles Ziss is a resident and citizen of Somerset County, New Jersey. Plaintiff Ziss' PII/PHI was provided to or obtained by Defendant in connection with its provision of medical treatment and services. Believing Defendant would implement and maintain reasonable security practices to protect his PII/PHI, Plaintiff Ziss routinely provided his PII/PHI to Defendant in connection with receiving medical treatment and services.

62. Plaintiff Ziss is careful about sharing his PII/PHI and takes reasonable steps to protect his PII/PHI. Plaintiff Ziss has never knowingly transmitted unencrypted PII/PHI over the internet or other unsecured source. Plaintiff Ziss stores any documents containing PII/PHI in a safe and secure location and diligently chooses unique usernames and passwords for his online accounts.

63. At the time of the Data Breach, Defendant retained Plaintiff Ziss' PII/PHI in its systems, and on information and belief, it continues to retain that information.

64. Plaintiff Ziss first learned of the Data Breach after receiving a Notice Letter from Defendant dated May 23, 2024, notifying him of the Data Breach and that his PII/PHI had been improperly accessed and disclosed to unauthorized third parties. This Notice Letter confirmed that his name, date of birth, mailing address, SSN, medical treatment information, and health insurance claims information may have been included in the compromised database.

65. Upon receiving notice of the Data Breach, Plaintiff Ziss made reasonable efforts to mitigate its impact, including, but not limited to, verifying the legitimacy of the Notice Letter and monitoring his bank accounts.

66. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Ziss will

need to maintain these heightened measures for years.

67. In the time following the Data Breach, Plaintiff Ziss has experienced an increase in spam texts and phone calls.

68. Plaintiff Ziss also suffered actual injury from having his PII/PHI compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential PII/PHI—a form of property that was entrusted to Defendant and was compromised as a result of the Data Breach Defendant failed to prevent, and (b) a violation of Plaintiff's privacy rights as a result of unauthorized disclosure of his PII/PHI.

69. Plaintiff Ziss has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because Defendant disclosed his PII/PHI to unauthorized parties who may now use that information for improper and unlawful purposes.

70. Plaintiff Ziss is exposed, and will continue to be exposed for the remainder of his life, to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his PII/PHI being obtained by unauthorized third parties and/or cybercriminals.

71. Plaintiff Ziss is also at a continued risk of harm because, on information and belief, his PII/PHI remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the PII/PHI in its possession.

72. Plaintiff Ziss has a continuing interest in ensuring that his PII/PHI, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks.

Plaintiff MaryAnn Joyce

73. Plaintiff MaryAnn Joyce is a resident and citizen of Wharton, New Jersey. Plaintiff Joyce's PII/PHI was provided to or obtained by Defendant in connection with its provision of medical of treatment and services. Believing Defendant would implement and maintain reasonable security practices to protect her PII/PHI, Plaintiff Joyce routinely provided her PII/PHI to Defendant in connection with receiving medical treatment and services.

74. Plaintiff Joyce is careful about sharing her PII/PHI and takes reasonable steps to protect her PII/PHI. Plaintiff Joyce has never knowingly transmitted unencrypted PII/PHI over the internet or other unsecured source. Plaintiff Joyce stores any documents containing PII/PHI in a safe and secure location and diligently chooses unique usernames and passwords for her online accounts.

75. At the time of the Data Breach, Defendant retained Plaintiff Joyce's PII/PHI in its systems, and on information and belief, it continues to retain that information.

76. Plaintiff Joyce first learned of the Data Breach after receiving a Notice Letter from Defendant dated May 23, 2024, notifying her of the Data Breach and that her PII/PHI had been improperly accessed and disclosed to unauthorized third parties. This Notice Letter confirmed that her name, date of birth, mailing address, SSN, medical treatment information, and health insurance claims information may have been included in the compromised database.

77. Upon receiving notice of the Data Breach, Plaintiff Joyce made reasonable efforts to mitigate its impact, including, but not limited to, updating and checking her credit monitoring services, reviewing her account statements weekly, changing passwords, adding alerts and multi-factor authentication to her accounts, and canceling and changing payment cards. These actions by

unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

78. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff Joyce will need to maintain these heightened measures for years.

79. In the time following the Data Breach, Plaintiff Joyce has experienced an increase in spam emails, calls and text messages as a result of the Data Breach, many of which are actively seeking to steal money and information from her.

80. Plaintiff Joyce also suffered actual injury from having her PII/PHI compromised as a result of the Data Breach, including, but not limited to: (a) damage to and diminution in the value of Plaintiff's confidential PII/PHI—a form of property that was entrusted to Defendant and was compromised as a result of the Data Breach Defendant failed to prevent, and (b) a violation of Plaintiff's privacy rights as a result of unauthorized disclosure of his PII/PHI.

81. Plaintiff Joyce has and is continuing to experience fear, stress, frustration, and anxiety, among other issues, because Defendant disclosed his PII/PHI to unauthorized parties who may now use that information for improper and unlawful purposes.

82. Plaintiff Joyce is exposed, and will continue to be exposed for the remainder of her life, to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her PII/PHI being obtained by unauthorized third parties and/or cybercriminals.

83. Plaintiff Joyce is also at a continued risk of harm because, on information and belief, her PII/PHI remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and is subject to further attack, so long as Defendant fails

to undertake the necessary and appropriate data security measures to protect the PII/PHI in its possession.

84. Plaintiff Joyce has a continuing interest in ensuring that her PII/PHI, which remains within Defendant's possession and control, is protected and safeguarded against future data breaches and cybersecurity risks.

85. As a result of Defendant's conduct, all Plaintiffs and Class Members suffered actual damages, including, without limitation, incurring time and expenses related to monitoring their financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of their PII/PHI, and other economic and non-economic harm. Plaintiffs will now be forced to expend additional time reviewing their credit reports and monitoring their financial accounts and medical records for fraud or identity theft—particularly since the compromised information may include confidential medical information.

Defendant

86. Defendant is a corporation organized under the laws of New Jersey with its principal place of business located at 182 South Street, Suite 1, Morristown, New Jersey 07960. Defendant provides a range of medical and cosmetic services to patients, including skin cancer screenings, Mohs microsurgery, acne treatment, eczema treatment, phototherapy, Botox, chemical peels, and micro-needling.[4]

JURISDICTION AND VENUE

87. This Court has jurisdiction over the subject matter of this action because the amount in controversy exceeds the sum of $20,000.

[4] *Home*, AFFILIATED DERMATOLOGISTS, https://www.affiliateddermatologists.com/ (last accessed Sept. 27, 2024).

88. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in New Jersey, the conduct giving rise to this action occurred in Morris County, New Jersey, and Defendant otherwise has substantial contacts with New Jersey and purposely availed itself of the courts of New Jersey.

89. Venue is proper in Morris County under R. 4:3-2(b) because Defendant's principal place of business is located in Morris County, and a substantial part of the events or omissions giving rise to the claims occurred in, were directed to, and/or emanated from Morris County.

FACTUAL ALLEGATIONS

Background and Overview of Defendant

90. As previously alleged, Defendant is a New Jersey-based dermatological healthcare practice group headquartered in Morristown, New Jersey, with additional locations in Arlington and Bridgewater, New Jersey.

91. Defendant provides a range of medical and cosmetic services to patients.[5]

92. In the regular course of its business, Defendant collects and maintains the PII/PHI of its patients, employees, and other individuals to whom it is currently providing or previously provided health-related services.

93. As a regular part of its business, Defendant requires patients and employees to provide PII/PHI in order to provide its services. That information includes, *inter alia*, names, dates of birth, SSN, medical treatment information, health insurance claims information, driver's license numbers and passport numbers. Defendant stores this information digitally.

94. Plaintiffs and Class Members provided their PII/PHI to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its

[5] *Id.*

obligations to keep such information confidential and secure from unauthorized access.

95. As a result of collecting and storing the PII/PHI of Plaintiffs and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiffs' and the Class Members' PII/PHI from disclosure to third parties.

Defendant Had a Duty to Protect Plaintiffs' PII/PHI

96. Upon information and belief, Defendant made promises and representations to its patients, including Plaintiffs and Class Members, that the PII/PHI collected from them would be kept safe, confidential, and that the privacy of that information would be maintained.

97. For instance, Defendant's website contains a page entitled "Patient Privacy," wherein Defendant ensures consumers that "the privacy of [their] medical information is important to [Defendant]."[6] Defendant also assures adherence to privacy or security rules when processing personal data on behalf of consumers or in relation to the provision of Defendant's services, stating in part:

Our legal duty

> We are required by applicable federal and state laws to maintain the privacy of your protected health information. We are also required to give you this notice about our privacy practices, our legal duties, and your rights concerning your protected health information.[7]

98. Defendant owed a duty to Plaintiffs and the Class to design, maintain, and test its computer and application systems to ensure that the PII/PHI in its possession was adequately secured and protected.

99. Defendant owed a duty to Plaintiffs and the Class to create and implement

[6] *Patient Privacy*, AFFILIATEDDERMATOLOGISTS.COM, https://www.affiliateddermatologists.com/disclaimers/patientprivacy/ (last accessed Sept. 27, 2024).
[7] *Id.*

reasonable data security practices and procedures to protect the PII/PHI in its possession, including adequately training its employees (and others who accessed PII/PHI within its computer systems) on how to adequately protect PII/PHI.

100. Defendant owed a duty to Plaintiffs and the Class to implement processes that would detect a breach on its systems in a timely manner.

101. Defendant owed a duty to Plaintiffs and the Class to act upon data security warnings and alerts in a timely fashion.

102. Defendant owed a duty to Plaintiffs and the Class to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII/PHI from theft because such an inadequacy would be a material fact in the decision to entrust PII/PHI with Defendant.

103. Defendant owed a duty to Plaintiffs and the Class to disclose in a timely and accurate manner when data breaches occurred.

104. Defendant owed Plaintiffs and Class Members a duty to take all reasonable and necessary measures to keep the PII/PHI it collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the PII/PHI, yet breached its duty by failing to implement or maintain adequate security practices.

The Data Breach

105. On or around March 5, 2024, Defendant detected unusual activity on several of its IT systems[8], and found a ransom note on it network indicating that its network had been breached and data was stolen.[9]

[8] Notice Letter, n.1, *supra.*
[9] Steven Adler, *New Jersey Dermatology Practice Suffers 380,000-Record Data Breach*, THE HIPAA JOURNAL (May 15, 2024), https://www.hipaajournal.com/new-jersey-affiliated-dermatologists-breach/.

106. On April 10, 2024, Defendant's internal investigation determined that between March 2, 2024, and March 5, 2024, the unauthorized actor obtained access to certain systems and copied data from its IT network, including the PII/PHI of patients and employees.[10]

107. In its Notice Letter, Defendant states that the following types of PII/PHI were compromised in the Data Breach: (1) names, (2) dates of birth, (3) mailing addresses, (4) SSNs, (5) driver's license numbers, (6) medical treatment information, and (7) health insurance information.[11]

108. All in all, approximately 373,000 individuals with information stored on Defendant's system had their PHI/PII breached.[12]

109. The notice that Defendant posted on its website on or around May 23, 2024, states the information that was accessed included:

> For certain patients: name, date of birth, mailing address, SSN, medical treatment information, and health insurance claims information.
>
> For certain employees: name, date of birth, mailing address, SSN, driver's license number, and passport number.[13]

110. Omitted from any of Defendant's notices were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII/PHI remains protected. Rather, Defendant has released only vague statements indicating that it discovered that "an unauthorized third party gained access and left a ransom note on Defendant's network" and

---

[10] *Id.*
[11] *Id.*
[12] Data Breach Notifications, OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/8a407012-92e1-4705-a2bd-2d388c523940.shtml (last accessed October 7, 2024).
[13] Notice Letter, n.1, *supra.*

that it has "moved quickly to investigate, respond, and confirm the security of [its] systems" and "has taken steps to further enhance its network security."[14]

111. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

112. Despite internally confirming the Data Breach on March 5, 2024, Defendant did not begin directly notifying affected individuals that their personal and health information was compromised until May 23, 2024.

113. While Defendant sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive PII/PHI of Plaintiffs and Class Members.

114. Defendant's delay in notifying patients and employees affected by the Data Breach violated the provisions of N.J. Stat. § 56:8-163, specifically the reporting provision which required Defendant, once it knew or had reason to know of a data security breach involving personal information affecting New Jersey residents, to provide notice of such breach "in the most expedient time possible and without unreasonable delay."

115. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted PII/PHI of Plaintiffs and Class Members, including their names, dates of birth, SSNs, medical treatment information, health insurance claims information, driver's license numbers, and passport numbers. Plaintiffs' and Class Members' PII/PHI was accessed and stolen in the Data Breach.

[14] Notice Letter, n.1, *supra*.

116. Plaintiffs further believe their PII/PHI, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

117. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

118. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures in order to protect its patients' and employees' PHI/PII.

Defendant Failed to Follow FTC Guidelines

119. Defendant is prohibited by the FTC Act, 15 U.S.C. § 45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

120. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[15]

121. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of PII/PHI that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[16]

122. The FTC further recommends that companies not maintain PHI/PII longer than is

[15] *Start with Security – A Guide for Business*, UNITED STATES FEDERAL TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[16] *Protecting Personal Information: A Guide for Business*, UNITED STATES FEDERAL TRADE COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

needed for authorization of a transaction; limit access to private 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.[17]

123. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer 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 FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

124. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[18] Immediate notification of a Data Breach is critical so that those impacted can take measures to protects themselves.

125. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PHI/PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

126. Defendant was at all times fully aware of its obligations to protect patients' PHI/PII because of its position as a healthcare provider, which gave it direct access to reams of patient PHI/PII. Defendant is also aware of the significant repercussions that would result from its failure to do so.

127. Despite its own knowledge of the inherent risks of cyberattacks, and

[17] *Id.*
[18] *Id.*

notwithstanding the FTC's data security principles and practices,[19] Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard its past and present patients' and employees sensitive PII/PHI.

Defendant Failed to Comply with Industry Standards for Data Security

128. In light of the evident threat of cyberattacks seeking consumers' PII/PHI, several best practices have been identified by regulatory agencies and experts that, at a minimum, should be implemented by companies within the healthcare industry, like Defendant, to secure Plaintiffs' and Class Members' PII/PHI.

129. Defendant is aware of the importance of safeguarding Plaintiffs' and Class Members' PII/PHI, and that by virtue of its business as a healthcare provider it placed Plaintiffs' and Class Members' PII/PHI at risk of being targeted by cybercriminals.

130. Because Defendant failed to implement, maintain, and comply with necessary cybersecurity requirements, as a result, it was unable to protect Plaintiffs' and Class Members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality.

131. Several best practices have been identified that at a minimum should be implemented by healthcare entities like Defendant, including, but not limited to: educating all employees; strong passwords; multi-layer security, such as firewalls and anti-virus and anti-malware software; encryption (e.g., making data unreadable without a key); multi-factor authentication; backup data; and limiting the number of employees with access to sensitive data.

132. Other commonly accepted data security standards among businesses that store personal information, such as the PII/PHI involved here, include, but are not limited to:

[19] *Id.*

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for personal and financial information;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

133. Defendant failed to meet the minimum standards of, e.g., the NIST Cybersecurity Framework, and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established industry standards in reasonable cybersecurity readiness.

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

135. Despite Defendant's obligations, Defendant failed to appropriately monitor and maintain its data security systems in a meaningful way so as to prevent the Data Breach.

136. Had Defendant properly maintained its systems and adequately protected them, it could have prevented the Data Breach.

PII/PHI Is Inherently Valuable

137. The PII/PHI that Defendant allowed to be exposed in the Data Breach is the type of valuable information that Defendant knew or should have known would be the target of cyberattacks.

138. Sensitive PII/PHI —like the SSNs and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals.

139. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2024 report, the healthcare compliance company Protenus found that there were 1,161 medical data breaches in 2023 with over 171 million patient records exposed.[20] This is an increase from the 1,138 medical data breaches which exposed approximately 59 million records that Protenus compiled in 2023.[21]

140. PII/PHI is a valuable property right.[22] The value of PII/PHI as a commodity is measurable.[23] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[24] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

141. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This

---

[20] *See 2024 Breach Barometer*, PROTENUS 2, https://protenus.com/hubfs/Breach_Barometer/Latest%20Version/Protenus%20-%20Industry%20Report%20-%20Privacy%20-%20Breach%20Barometer%20-%202024.pdf (last accessed Sept. 27, 2024).

[21] *See id*.

[22] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[23] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[24] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

142. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[25] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[26] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[27]

143. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[28] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen SSN or credit card number.[29]

144. John Riggi, the American Hospital Association National Advisor for Cybersecurity and Risk, said "foreign cyber gangs and spies" were testing the resilience of hospitals especially

---

[25] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").
[26] *Id.*
[27] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.
[28] SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.
[29] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

as hospitals began to fill up at the time because of the "tripledemic" including increased cases of RSV, flu and COVID-19.[30]

145. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[31] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[32]

146. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[33]

147. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

The Data Breach Was a Foreseeable Risk

148. The Data Breach was foreseeable and avoidable.

149. Various governmental bodies have put entities like Defendant on notice of the likelihood of cyberattacks. In a Joint Cybersecurity Advisor, the FBI and the Cybersecurity &

---

[30] Dan Alexander, *Personal Data of 617,000 Patients Exposed in NJ Hospital Cyberattack*, NEW JERSEY 101.5 (Feb. 13, 2023), https://nj1015.com/personal-data-of-617000-patients-exposed-in-nj-hospital-cyberattack/.
[31] *What Happens to Stolen Healthcare Data* Article, n.25, *supra*.
[32] *Id.*
[33] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

Infrastructure Security Agency ("CISA") encouraged critical infrastructure organizations, such as Defendant, to implement their various recommendations as set forth in the advisory to reduce the likelihood and impact of inevitable ransomware and data extortion efforts, including against similar ransomware attacks perpetrated by similar ransomware gangs.[34]

150. Indeed, cyberattacks have been common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[35]

151. Cyberattacks have become so notorious that the 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."[36]

152. The Office for Civil Rights ("OCR") also urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, OCR's deputy director of health

---

[34] *See, e.g*, *#StopRansomware: ALPHV Blackcat*, AMERICA'S CYBER DEFENSE AGENCY (Feb. 27, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a; *#StopRansomware: ALPHV Blackcat*, AMERICA'S CYBER DEFENSE AGENCY (May 10, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a.

[35] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[36] 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.

information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[37]

153. Moreover, in light of recent high profile data breaches at other industry leading companies, including, Ticketmaster (560 million records, May 2024), AT&T (73 million records, March 2024), MOVEit, (77 million records, 2023), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII/PHI that they collected and maintained would be targeted by cybercriminals.

154. Data breaches are preventable. As Lucy Thompson wrote in the *Data Breach and Encryption Handbook*, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[38] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised…" and "[m]ost of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … [a]ppropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."[39]

155. Additionally, as a HIPAA-covered entity handling PII/PHI, Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and

---

[37] *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (Apr. 22, 2014), https://wayback.archiveit.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.
[38] Lucy L. Thompson, *Data Breach and Encryption Handbook* (Lucy Thompson, ed., 2011) https://archive.org/details/isbn_9781604429893/page/28/mode/2up.
[39] *Id*.

data breaches in the healthcare industry, and other industries holding significant amounts of PII and personal health information, preceding the Data Breach. Defendant's status as a healthcare provider and, therefore, a HIPAA-covered entity should have put Defendant on high alert as to the importance of its data security obligations.

156. Healthcare-related breaches, in particular, have continued to rapidly increase because electronic patient data is seen as a valuable asset. In fact, entities that store patient information "have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[40]

157. Healthcare entities suffer data breaches at an alarming rate. In 2023, an average of about 2 healthcare data breaches of 500 or more records were reported *each day*, and on average, 364,571 healthcare records were breached every day.[41] In 2023, more than 133 million records were exposed or impermissibly disclosed.[42]

158. According to the HIPAA Journal's 2023 Healthcare Data Breach Report, "[a]n unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services Office for Civil Rights, beating the record of 720 healthcare security breaches set the previous year."[43]

---

[40] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, CHIEF HEALTHCARE EXECUTIVE (Apr. 4, 2019), https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

[41] Steve Alder, *Healthcare Data Breach Statistics*, THE HIPAA JOURNAL (Sept. 24, 2024) https://www.hipaajournal.com/healthcare-data-breach-statistics/#:~:text=In%202023%2C%20an%20average%20of,records%20were%20breached%20every%20day.

[42] *Id*.

[43] Steve Alder, *Security Breaches in Healthcare in 2023*, THE HIPAA JOURNAL (Jan. 31, 2024), www.hipaajournal.com/wp-

159. 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. For this reason, Defendant knew or should have known about these dangers and strengthened its data security 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.

160. Defendant was well aware that the protected PII/PHI it acquires, stores, and utilizes is highly sensitive and of significant value to both the owners of the PII/PHI and those who would use it for wrongful purposes.

161. Defendant knew, or should have known, the importance of safeguarding the PII/PHI entrusted to it and of the foreseeable consequences if its systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

162. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII/PHI of Plaintiffs and Class Members from being compromised.

163. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII/PHI of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

164. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's servers, amounting to potentially hundreds of thousands

---

content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf.

of individuals' detailed PII/PHI, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

165. As a highly sophisticated party that handles sensitive PII/PHI, Defendant failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and other Class Members' PII/PHI to protect against anticipated threats of intrusion of such information.

166. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in industries holding significant amounts of PII preceding the date of the breach.

The Data Breach Put Plaintiffs and Class Members at an Increased Risk of Fraud and Identity Theft

167. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[44]

168. Identity thieves use PII/PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[45] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new

[44] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER ADVICE, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Oct. 7, 2024).

[45] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[46]

169. With access to PII/PHI, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and even give victim's personal information to police during an arrest, resulting in an arrest warrant being issued in victim's name.[47]

170. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[48]

171. SSNs are particularly sensitive pieces of personal information. With a stolen SSN, which is only one subset of the PHI/PII compromised in the Data Breach, someone can open

---

[46] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[47] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed May 8, 2024).

[48] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[49]

172. The Social Security Administration have warned that identity thieves can use an individual's SSN to apply for additional credit lines.[50] Such fraud may go undetected until debt collection calls commence months, or even years, later. SSNs also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[51] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her SSN was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected because one was already filed on their behalf.

173. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. To obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of his SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

174. An individual cannot obtain a new SSN without significant paperwork and evidence of actual misuse. Even then, a new SSN may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[52]

175. Theft of drivers' license numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced.

---

[49] *Id.*
[50] *Id.*
[51] *Id.* at 4.
[52] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

176. The theft of drivers' license numbers in combination with other PII (e.g., name, address, date of birth) can result in a variety of fraudulent activity.

177. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[53] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[54] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [55] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[56]

178. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

---

[53] Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), https://www.ftc.gov/system/files/documents/public_comments/2018/01/00037-142815.pdf.
[54] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk*…, *supra* at n.29.
[55] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Oct. 7, 2024).
[56] *Id*.

- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

- Phantom medical debt collection based on medical billing or other identity information.

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[57]

179. There may also be a time lag between when sensitive PII/PHI is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[58]

180. According to the GAO, 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.[59]

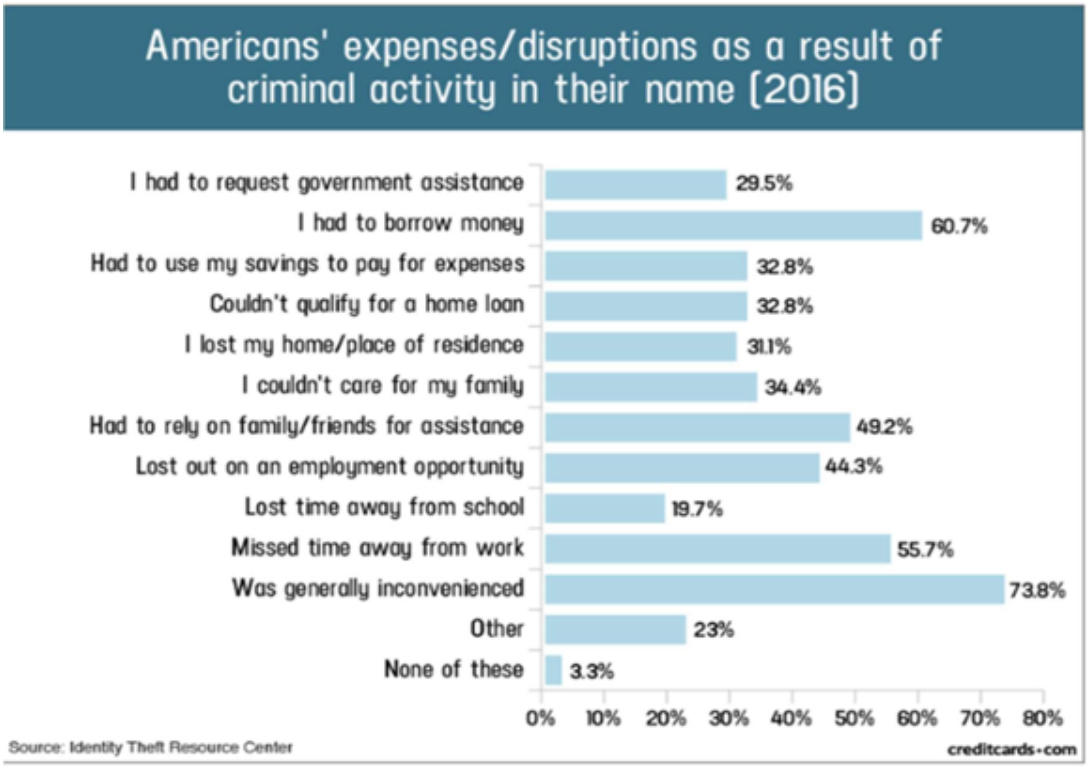
181. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. As with income tax returns, an individual may not know that his or her SSN was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud.

---

[57] *See The Geography of Medical Identity Theft*, *supra* at n.53.
[58] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.
[59] *Id.*

182. In fact, approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[60] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[61]

183. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.



[60] *See* Medical ID Theft Checklist, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last accessed Sept. 27, 2024).
[61] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches*, EXPERIAN, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last accessed Apr. 17, 2023).

184. Victims of the Data Breach, like Plaintiffs, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[62]

185. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[63]

186. It is within this context that Plaintiffs and all other Class Members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

187. 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. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to 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. 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 SSN. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into

---

[62] *Id.*

[63] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Feb. 17, 2023).

disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

188. As a direct and proximate result of the Data Breach, Plaintiffs had their PHI/PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

189. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PHI/PII, which remains in the possession of Defendant is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiffs' PHI/PII.

190. Plaintiffs and Class Members also have an interest in ensuring that their PII/PHI that was provided to Defendant is removed from Defendant's unencrypted files.

Plaintiffs and Class Members Suffered and Are Suffering Damages

191. Defendant disregarded the rights of Plaintiffs and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to

adequately safeguard Plaintiffs and Class Members' PII/PHI; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

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

193. Plaintiffs had a reasonable expectation of privacy while receiving medical services. Plaintiffs would not have agreed to have their sensitive PII/PHI provided to and maintained by Defendant had they known that Defendant would fail to adequately protect the PII/PHI. Indeed, Plaintiffs sought medical care through Defendant with the reasonable expectation that Defendant would keep PII/PHI secure and inaccessible to unauthorized parties. Plaintiffs and Class Members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their PII/PHI from criminal theft and misuse.

194. Defendant knew, or reasonably should have known, of the importance of safeguarding PII/PHI and of the foreseeable consequences that would result if Plaintiffs' and Class

Members' PII/PHI were stolen, including the significant costs that would be placed on Plaintiffs and Class Members as a result of the breach.

195. The risk of improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendant, and Defendant was on notice that failing to take necessary steps to secure Plaintiffs' and Class Members' PII from that risk left the PII in a dangerous condition.

196. As a result of Defendant's failure to implement and follow even the most basic security procedures, Plaintiffs and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including, but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

d. The imminent and certainly impending risk of having their confidential PII used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class Members' PII for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

197. Plaintiffs and Class Members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiffs and Class Members have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Data Breach.

198. Plaintiffs and Class Members further have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing “freezes” and “alerts” with reporting agencies;

d. Spending time on the phone with or at financial institutions and/or government agencies to dispute unauthorized and fraudulent activity in their names;

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

f. Closely reviewing and monitoring insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

199. Further, because Defendant delayed in discovering and notifying Plaintiffs about the Data Breach, Plaintiffs were unable to take affirmative steps during that time period to attempt to mitigate any harm or take prophylactic steps to protect against injury.

200. This caused Plaintiffs to be at a continued risk because their information remains in Defendant's computer systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fail to undertake the necessary and appropriate security and training measures to protect its patients' PHI/PII.

201. Once PHI/PII is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

202. Identity theft is the most common consequence of a data breach—it occurs to 65% of data breach victims.[64] Consumers lost more than $56 billion to identity theft and fraud in 2020, and over 75% of identity theft victims reported emotional distress.[65]

203. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those

[64] Eugene Bekker, *What Are Your Odds of Getting Your Identity Stolen?*, IDENTITYFORCE BLOG (Apr. 14, 2021), https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics.
[65] *Id*.

affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[66]

204. Stolen PII/PHI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

205. When malicious actors infiltrate companies and steal PII/PHI, the stolen information often ends up on the dark web because those actors buy and sell that information for profit.[67]

206. According to the FBI's Internet Crime Complaint Center (IC3) 2023 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2023, resulting in more than $12.5 billion in losses to individuals and business victims.[68]

207. Further, according to the same report, reporting incidents rapidly is essential: "[b]y reporting the incident, the FBI may be able to provide information on decryption, recover stolen data, possibly seize/recover ransom payments, and gain insight on adversary tactics."[69] Defendant did not rapidly report to Plaintiffs and Class Members that their PII/PHI had been stolen.

208. In addition to a remedy for economic harm, Plaintiffs and Class Members maintain an interest in ensuring that their PII/PHI is secure, remains secure, and is not subject to further misappropriation and theft.

---

[66] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud.
[67] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Feb. 1, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring.
[68] *2023 Internet Crime Report Released*, FBI https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (last accessed Sept. 27, 2024).
[69] *Id.*

209. Cyberattacks and data breaches can also negatively impact the overall daily lives of individuals affected by the attack.

210. Researchers have found that among companies that handle healthcare information that experience a data security incident, the death rate among patients increased in the months and years after the attack.[70]

211. Researchers have further found that after a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[71]

212. Plaintiffs and Class Members face a substantial risk of identity theft given that their SSNs, addresses, dates of birth, and other important PII/PHI were compromised in the Data Breach. Once an SSN is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

213. 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 face "substantial costs and time to repair the damage to their good name and credit record."[72]

214. The PII exposed in the Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein.

215. This was a financially motivated data breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Defendant is to

---

[70] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour /science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[71] *See* Sung J. Choi, et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 HEALTH SERVICES RESEARCH 971, 971-980 (2019), https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[72] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, (June 2007), https://www.gao.gov/new.items/d07737.pdf.

get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

216. Indeed, an SSN, date of birth, and full name can sell for high prices on the digital black market.[73] "[I]f there is reason to believe that your personal information have been stolen, you should assume that it can end up for sale on the dark web."[74]

217. These risks are both certainly impending and substantial. As the FTC have reported, if hackers get access to PHI/PII, they *will use it.*[75]

218. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[76]

219. Victims of the Data Breach, like Plaintiffs and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[77] The Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

---

[73] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.
[74] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[75] *Id.*
[76] *Guide for Assisting Identity Theft Victims*, FED. TRADE COMM'N, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.
[77] *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), http://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

CLASS ALLEGATIONS

220. This action is brought and may be properly maintained as a class action pursuant to New Jersey Rules of Court 4:32.

221. Plaintiffs bring this action individually and on behalf of all members of the following Classes of similarly situated persons:

> Nationwide Class
>
> All natural persons who are residents of the United States whose PII/PHI was compromised in the Data Breach disclosed by Defendant, including all who were sent a Notice Letter.
>
> New Jersey Class
>
> All natural persons who are residents of New Jersey whose PII/PHI was compromised in the Data Breach disclosed by Defendant, including all who were sent a Notice Letter.

222. Excluded from the Class are: (1) the Judges presiding over this action and members of their immediate families and their staff; (2) Defendant, its subsidiaries, parent companies, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and its current or former officers and directors.

223. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

224. The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. Defendant reported that the Data Breach involved the personal and health information of approximately 373,379 individuals.

225. Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII/PHI;

c. Whether an implied contract existed between Class Members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Plaintiffs' and Class Members' PII/PHI from unauthorized access and disclosure;

d. Whether Defendant breached its duties to protect Plaintiffs' and Class Members' PII/PHI; and

e. Whether Plaintiffs and all other Class Members are entitled to damages and the measure of such damages and relief.

226. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, individually and on behalf of all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

227. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII/PHI compromised in the Data Breach. Plaintiffs and Class Members were injured by the same wrongful acts, practices, and omissions committed by

Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

228. Plaintiffs will fairly and adequately protect the interests of all Class Members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

229. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class Members to individually seek redress from Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the New Jersey Class)

230. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

231. Defendant owed a duty to Plaintiffs and all other Class Members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

232. Defendant knew the risks of collecting and storing Plaintiffs' and all other Class Members' PII/PHI and the importance of maintaining secure systems. Defendant knew of the many data breaches that targeted healthcare providers in recent years.

233. Given the nature of Defendant's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

234. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to them—including Plaintiffs' and Class Members' PII/PHI.

235. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class Members' PII/PHI to unauthorized individuals.

236. But for Defendant's negligent conduct or breach of the above-described duties owed to Plaintiffs and Class Members, their PII/PHI would not have been compromised.

237. As a result of Defendant's above-described wrongful actions, inaction, and want of

ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach.

COUNT II
NEGLIGENCE PER SE
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the New Jersey Class)

238. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

239. Defendant's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

240. Defendant's duties also arise from Section 5 of the FTC Act, 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendant, of failing to employ reasonable measures to protect and secure PII/PHI.

241. In addition, NJ Rev. Stat. § 26:2J-27 requires that all medical facilities, such as

those operated by Defendant, ensure that medical records and communications are kept confidential.

242. Defendant violated HIPAA Privacy and Security Rules and Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and all other Class Members' PII/PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiffs and the other Class Members.

243. Defendant's violation of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

244. Plaintiffs and Class Members are within the class of persons the HIPAA Privacy and Security Rules and Section 5 of the FTC Act were intended to protect.

245. The harm occurring as a result of the Data Breach is the type of harm the HIPAA Privacy and Security Rules and Section 5 of the FTC Act were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and all other Class Members as a result of the Data Breach.

246. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would

result in the release, disclosure, and dissemination of Plaintiffs' and Class Members' PII/PHI to unauthorized individuals.

247. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Defendant's violations of HIPAA Privacy and Security Rules and Section 5 of the FTC Act. Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach.

COUNT III
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the New Jersey Class)

248. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

249. Plaintiffs and Class Members provided Defendant, their healthcare provider, with their PII/PHI in confidence, believing that Defendant would protect that information. Plaintiffs and Class Members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's role as Plaintiffs' and Class Members' healthcare provider, as well as its acceptance and storage of Plaintiffs' and Class Members' PII/PHI, created a fiduciary relationship between Defendant, on the one hand, and Plaintiffs and Class Members,

on the other hand. In light of this relationship, Defendant is obligated to act primarily for the benefit of its patients and employees, which includes safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

250. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. Defendant breached that duty by failing to properly protect the integrity of its systems containing Plaintiffs' and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Class Members' PII/PHI that it collected.

251. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the New Jersey Class)

252. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

253. In connection with receiving medical treatment, services, and/or employment with Defendant, Plaintiffs and all other Class Members entered into implied contracts with Defendant.

254. Pursuant to these implied contracts, Plaintiffs and Class Members paid money to Defendant, whether directly or indirectly, and provided Defendant with their PII/PHI. In exchange, Defendant agreed to, among other things, and Plaintiffs and Class Members understood that Defendant would: (1) provide medical treatment, services, health plan benefits, and/or employment to Plaintiffs and Class Members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' PII/PHI; and (3) protect Plaintiffs' and Class Members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

255. The protection of PII/PHI was a material term of the implied contracts between Plaintiffs and Class Members, on the one hand, and Defendant, on the other hand. Indeed, as set forth *supra*, Defendant recognized the importance of data security and the privacy of its patients' PII/PHI in, *inter alia*, Patient Privacy page and notice. Had Plaintiffs and Class Members known that Defendant would not adequately protect their PII/PHI, they would not have provided Defendant with their PII/PHI and/or obtained medical treatment or services or employment from Defendant.

256. Plaintiffs and Class Members performed their obligations under the implied contract when they provided Defendant with their PII/PHI and paid—directly or indirectly—for health care treatment or other services from Defendant.

257. Defendant breached its obligations under its implied contracts with Plaintiffs and Class Members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class Members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

258. Defendant's breach of its obligations of their implied contracts with Plaintiffs and Class Members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class Members have suffered from the Data Breach.

259. Plaintiffs and all other Class Members were damaged by Defendant's breach of implied contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT V
INVASION OF PRIVACY/INTRUSION UPON SECLUSION
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the New Jersey Class)

260. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

261. Plaintiffs and Class Members had a reasonable expectation of privacy in the PII/PHI that Defendant disclosed without authorization.

262. Defendant's conduct intruded upon Plaintiffs' and Class Members' seclusion under common law.

263. By failing to keep Plaintiffs' and Class Members' PII/PHI safe, knowingly employing inadequate data privacy policies and protocols, and disclosing PII/PHI to unauthorized

parties for unauthorized use, Defendant unlawfully invaded Plaintiffs' and Class Members' privacy by, *inter alia*:

a. intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; and

b. invading Plaintiffs' and Class Members' privacy by improperly using their PII/PHI properly obtained for a specific purpose for another purpose, or disclosing it to some third party;

c. failing to adequately secure PII/PHI from disclosure to unauthorized persons;

d. enabling the disclosure of Plaintiffs' and Class Members' PII/PHI without consent.

264. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider their actions highly offensive.

265. Defendant knew that its IT systems and servers were vulnerable to data breaches prior to the Data Breach.

266. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by disclosing their PII/PHI to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

267. As a proximate result of such unauthorized disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their PII/PHI was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiffs' and Class Members' protected privacy interests.

268. In failing to protect Plaintiffs' and Class Members' PII/PHI, and in disclosing Plaintiffs' and Class Members' PII/PHI, Defendant acted with malice and oppression and in

conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

269. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT VI
VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT
N.J.S.A. § 56:8-1, *et seq*.
(On behalf of Plaintiffs and the New Jersey Class)

270. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

271. Defendant has violated N.J.S.A. § 56:8-1*, et seq*., by engaging in unconscionable, deceptive, or fraudulent business acts and practices and omissions regarding the same as defined in N.J.S.A. § 56:8-2 with respect to the services provided to Plaintiffs and the New Jersey Class ("Class" for purposes of this cause of action).

272. Defendant engaged in unconscionable acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting the PII/PHI of Plaintiffs and the Class with knowledge that the information would not be adequately protected; and by storing the PII/PHI of Plaintiffs and the Class in an unsecure environment in violation of HIPAA and the rules and regulations promulgated thereunder, including 42 U.S.C. § 1301, *et seq*., 45 C.F.R. §§ 164.400-414, and 45 C.F.R. § 164.306, *et seq*. (as alleged *supra*.); and in violation of the Federal Trade Commission Act, 15 U.S.C. § 45 and 17 C.F.R. § 248.201, which require Defendant to employ reasonable methods of safeguarding the PII/PHI of Plaintiffs and the Class.

273. Further, Defendant failed to inform Plaintiffs and the Class that it had not undertaken sufficient measures to ensure the security of their PII/PHI.

274. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiffs and the Class were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Plaintiffs' and the Class's legally protected interest in the confidentiality and privacy of their PII/PHI, nominal damages, and additional losses as described above.

275. Defendant knew or should have known that its data security practices were inadequate to safeguard the PII/PHI of Plaintiffs and the Class and that the risk of a data breach or theft was highly likely, especially given its inability to adhere to basic encryption standards and data disposal methodologies. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Class.

276. Plaintiffs and the Class seek relief under N.J.S.A. § 56:8-2.12 and §56-8.19 including, but not limited to, restitution to Plaintiffs and the Class of money or property that Defendant may have acquired by means of Defendant's unconscionable business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unconscionable business practices, treble damages, declaratory relief, attorneys' fees and costs and injunctive or other equitable relief.

COUNT VII
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the New Jersey Class)

277. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

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

279. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of monies paid for healthcare services and/or performed employment services for Defendant.

280. Defendant accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members. Defendant also benefitted from the receipt of Plaintiffs' and Class Members' PII/PHI, as this information was used to facilitate payment for its services and/or employ Plaintiffs and Class Members.

281. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

282. Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

283. Defendant should be compelled to provide, for the benefit of Plaintiffs and Class Members, all unlawful proceeds received by it as a result of its misconduct and the Data Breach.

COUNT VIII
DECLARATORY RELIEF
(On behalf of Plaintiffs and the Nationwide Class, or, alternatively, the New Jersey Class)

284. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

285. The Declaratory Judgments Act, N.J.S.A. 2A:16-51 *et seq*. authorizes courts to

declare rights, status, and other legal relations so as to afford litigants relief from uncertainty and insecurity.

286. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective duties to reasonably safeguard Plaintiffs' and Class Members' PII/PHI, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their PII/PHI.

287. The Data Breach evidences Defendant's failure to provide security measures that were adequate, reasonable, and/or compliant with industry standards and best practices with regard to safeguarding Plaintiffs and Class Members' PII/PHI.

288. The Data Breach, and Defendant's response to the Data Breach, demonstrates that its systems remain vulnerable to unauthorized access, and more stringent measures must be taken to safeguard the PII/PHI of Plaintiffs and the Class Members going forward.

289. Plaintiffs seek a declaration that Defendant's current security measures are inadequate to safeguard PII/PHI, do not comply with its obligations to keep PII/PHI secure, and that Defendant must implement specific additional security practices to provide reasonable protection and security for the PII/PHI it maintains, including the PII/PHI of Plaintiffs and Class Members.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, individually and on behalf of the Class, seek appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

CERTIFICATION PURSUANT TO R. 4:5-1

I hereby certify that to the best of my knowledge, information, and belief at this time, the matter in controversy is the subject of no other actions in any court. I additionally certify that, to the best of my knowledge, information, and belief at this time, I am not aware of any other non-parties who should be joined in the action.

CERTIFICATION PURSUANT TO R. 1:38-7(c)

I hereby certify that confidential personal identifiers have been redacted from documents

now submitted to the Court and will be redacted from all documents in the future in accordance with R. 1:38-7(b).

TRIAL COUNSEL DESIGNATION

Please take notice that pursuant to the provisions of R. 4:25-4, Andrew Ferich, Mariya Weekes, Kristen Lake Cardoso, and Marc Edelson, are hereby designated as trial counsel on behalf of Plaintiffs.

Date: October 7, 2024

/s/ Andrew W. Ferich

Andrew W. Ferich (NJ 015052012)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: (310) 474-9111
Facsimile: (310) 474-8585
aferich@ahdootwolfson.com

Bradley K. King (NJ 081472013)
AHDOOT & WOLFSON, PC
521 5th Avenue, 17th Floor
New York, NY 10175
Telephone: (917) 336-0171
Facsimile: (917) 336-0177
bking@ahdootwolfson.com

Mariya Weekes (admitted *pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2nd Floor
Coral Gables, FL 33134
Telephone: (786) 879-8200
Facsimile: (786) 879-7520
mweekes@milberg.com

Kristen Lake Cardoso (admitted *pro hac vice*)
KOPELOWITZ OSTROW P.A.
1 West Las Olas Blvd., 5th Floor
Ft. Lauderdale, FL 33301
Telephone: (954) 525-4100
Facsimile: (954) 525-4300
cardoso@kolawyers.com

Marc H. Edelson (admitted *pro hac vice*)
EDELSON LECHTZIN LLP
411 S. State Street, Suite N-300
Newtown, PA 18940
Telephone: (215) 867-2399
Facsimile: (267) 685-0676
medelson@edelson-law.com

Interim Class Counsel