UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN RE HARVARD PILGRIM DATA SECURITY INCIDENT LITIGATION **This Document relates to: All Cases**	**Case No. 1:23-cv-11211-NMG** **CLASS ACTION** **JURY TRIAL DEMAND**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Madeline Docanto, Justin Dyer, Svea Elaine, Ruth Kidder, Daniel Neal, Danielle Olson, Girard Patterson, Tanya Peckham, Margaret Donovan, Angela Rountree, and Tracie Wilson, individually and on behalf of all others similarly situated (collectively, "Class Members"), by and through their attorneys, bring this action against Point32Health, Inc. ("Point32Health") and Harvard Pilgrim Health Care, Inc. ("Harvard Pilgrim") (collectively "Defendants"). The following allegations are based on Plaintiffs' knowledge, investigations of counsel, facts of public record, including Defendants' own statements, and information and belief.

NATURE OF THE ACTION

1. Plaintiffs seek to hold Defendants responsible for the substantial and largely irreparable injuries Defendants inflicted on Plaintiffs and at least 2,860,795[1] similarly situated persons ("Class Members") as a result of Defendants' unlawfully inadequate data security, which caused the personal information and personal health information of Plaintiffs and those similarly situated

[1] Office of the Maine Attorney General, Data Breach Notifications: Harvard Pilgrim Healthcare, https://apps.web.maine.gov/online/aeviewer/ME/40/f871258f-9014-4ef3-afa7-0208e4482bf1.shtml (last accessed April 26, 2024).

to be exfiltrated through unauthorized access by cybercriminals (the "Data Breach" or "Breach") between March 28, 2023, and April 17, 2023.[2]

2. The private information compromised in the Data Breach consisted of highly sensitive personal data, a veritable gold mine for data thieves. The data that Defendants caused—through negligence, recklessness, or intentional wrongdoing—to be exfiltrated by cybercriminals included private information, personal identifying information ("PII"), and personal health information ("PHI," and collectively with PII, "Private Information"), such as, but not limited to, individuals' names, physical addresses, phone numbers, dates of birth, health insurance account information, Social Security numbers, taxpayer-identification numbers, and clinical information (*e.g.*, medical history, diagnoses, treatment, dates of service, and provider names).While the breach was discovered by the Defendants on April 17, 2023, it was only on May 24, 2023, that Harvard Pilgrim, one of the largest health insurers in the Northeast United States, announced that it was advising more than 2.5 million affected individuals of a ransomware data breach attack that it had suffered in April 2023 at the hands of at least one third-party hacker.[3] In March 2024, Defendant Harvard Pilgrim updated the number of affected individuals to over *2.8* million.[4]

---

[2] *See* Harvard Pilgrim Health Care, Notice of Data Security Incident, available at https://www.harvardpilgrim.org/public/notice-of-data-security-incident (last accessed April 11, 2024).

[3] *Id*.

[4] Office of the Maine Attorney General, Data Breach Notifications: Harvard Pilgrim Healthcare, https://apps.web.maine.gov/online/aeviewer/ME/40/f871258f-9014-4ef3-afa7-0208e4482bf1.shtml (last accessed April 26, 2024); Ionut Arghire, Massachusetts Health Insurer Data Breach Impacts 2.8 Million, SecurityWeek, https://www.securityweek.com/massachusetts-health-insurer-data-breach-impacts-2-8-million/amp/ (Mar. 29, 2024).

3. Even when Defendants finally notified Plaintiffs and Class Members of the exfiltration of their Private Information, Defendants failed to adequately describe the Data Breach and its effects.

4. According to Defendants' own statements, all current or former members of Harvard Pilgrim (including individual and family plans purchased directly from Harvard Pilgrim, through state-based exchanges, or through plans selected through their employers) at any time between March 28, 2012, and April 17, 2023 – a period of over 10 years – were affected. Additionally, any consumers whose physician or other provider is currently contracted with Harvard Pilgrim were affected. Consumers may also have been affected if they are current or former members of certain additional Harvard Pilgrim-related health plans at any time between June 1, 2020, and April 17, 2023. Defendants' negligent, reckless, or intentional failure to adequately secure the private, personal medical information has grievously harmed Plaintiffs, Class Members, and all others similarly situated, including all persons who either are enrolled or were previously enrolled in Defendants' health plans and who were identified as individuals potentially affected by that breach by Defendants or by the U.S. Department of Health and Human Services Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information.

5. Plaintiffs and Class Members are at a significant risk of identity theft and many other forms of personal, social, and financial harm as the result of the Data Breach. These risks will continue for the remainder of their respective lifetimes.

6. Armed with the private information accessed in the Data Breach, data thieves can now commit a variety of crimes against Class Members including, but not limited to: (1) opening new financial accounts in Class Members' names; (2) taking out new loans in Class Members' names;

(3) using Class Members' names to obtain medical services; (4) using Class Members' information to obtain government benefits; (5) filing fraudulent tax returns using Class Members' information; (6) obtaining driver's licenses in Class Members' names but with another person's photograph; (7) and giving false information to police during an arrest. Each of these unauthorized uses of Class Members' personal information exposes them to significant financial, civil, and even criminal liability.

7. Defendants abdicated their legal obligations and duties to protect sensitive personal information in their possession and failed to take steps necessary to prevent the attack or mitigate its harm. Defendants have refused to date to fully and adequately notify victims of this attack that their personal information was improperly accessed and stolen because of the attack. Nor have Defendants provided appropriate relief. Based on information readily available to Defendants, and in view of the known threat of attacks against health systems and healthcare providers, this was an entirely foreseeable event that could and should have been prevented. Because of the negligent design of Defendants' networks, it was not.

8. Since the Private Information impacted in the Data Breach encompasses highly personal and revealing information, it is greatly valued by criminals as a golden ticket to medical identity theft and general identity theft. Private Information such as that wrongfully accessed in the Breach has been found to command up to $1,000 per individual victim on the dark web. Organizations such as Defendants who are entrusted with this most sensitive and valuable data have a non-delegable and fiduciary duty to take particularly special care to maintain up-to-date information security practices and keep apprised of industry-related threats as they arise.

9. The threat of such an attack was reasonably foreseeable to Defendants. Healthcare companies had been repeatedly warned of the potential for such an attack on their computer

systems. Defendants also were aware, or should have been aware, of the many health system and healthcare provider data breaches that have occurred over the last decade. Yet, Defendants and their employees ignored these warnings and failed to implement reasonable and adequate security procedures for protection of these data.

10. Defendants' failure to adequately protect the nonpublic Private Information in their possession has likely caused, and will continue to cause, substantial harm and injuries to Plaintiffs and Class Members. Plaintiffs and the Class are thus entitled to injunctive and other equitable relief.

11. Today, the privacy of Plaintiffs and Class Members has been compromised because of Defendants' unlawful dereliction of their non-delegable duties. Plaintiffs and Class Members now suffer from a present and continuing risk of harm, including fraud and identity theft, and must now constantly monitor their financial accounts.

12. Plaintiffs and Class Members have suffered—and will continue to suffer—from additional financial costs and loss of time for researching, purchasing, and/or putting in place necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Plaintiffs and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their Private Information, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the Data Breach.

14. Through this action, Plaintiffs seek to remedy these injuries on behalf of themselves and all similarly situated individuals whose Private Information were exfiltrated and compromised in the Data Breach.

15. Plaintiffs bring this action against Defendants and assert claims for negligence, negligence per se, unjust enrichment, breach of fiduciary duty, bailment, intrusion upon seclusion, breach of contract, violations of various state statutes, declaratory judgment and injunctive relief.

PARTIES

Plaintiff Madeline Docanto

16. Plaintiff Docanto is an adult individual and a natural person of Massachusetts, residing in Suffolk County, where she intends to stay.

17. Plaintiff provided her Private Information to Harvard Pilgrim as a condition of receiving health-related services. Upon information and belief, Plaintiff Docanto's Private Information was stored and maintained by Defendant Harvard Pilgrim.

18. Plaintiff Docanto received a notice letter from Defendant Harvard Pilgrim dated June 15, 2023 informing her of the Data Breach and the exposure of her Private Information.

19. The notice letter informed Plaintiff Docanto that her name, address, Social Security number phone number, date of birth, health insurance information, and clinical information (medical history, diagnoses, treatment, dates of service, and provider names) were potentially compromised in the Data Breach.

Plaintiff Justin Dyer

20. Plaintiff Dyer is an adult individual and a natural person of Maine, residing in Franklin County, where he intends to stay.

21. Plaintiff Dyer provided his and his minor children's Private Information to Harvard Pilgrim as a condition of receiving health-related services. Upon information and belief, Plaintiff Dyer's and his minor children's Private Information was stored and maintained by Defendant Harvard Pilgrim.

22. Plaintiff Dyer received notice letters from Defendant Harvard Pilgrim dated June 15, 2023 informing him of the Data Breach and the exposure of his and his minor children's Private Information.

23. The notice letters informed Plaintiff Dyer that his and his minor children's names, addresses, Social Security numbers, phone numbers, dates of birth, health insurance information, and clinical information (medical history, diagnoses, treatment, dates of service, and provider names) were potentially compromised in the Data Breach.

Plaintiff Svea Elaine

24. Plaintiff Svea Elaine is an adult individual and a natural person of Maine, residing in Kennebec County, where she intends to stay.

25. Plaintiff Elaine provided her Private Information to Harvard Pilgrim as a condition of receiving health-related services. Upon information and belief, Plaintiff Elaine's Private Information was stored and maintained by Defendant Harvard Pilgrim.

26. Plaintiff Elaine received a notice letter from Defendant Harvard Pilgrim dated June 15, 2023, informing her of the Data Breach and the exposure of her Private Information.

27. The notice letter informed Plaintiff Elaine that her name, physical address, phone number, date of birth, health insurance account information, Social Security number, and clinical information (medical history, diagnoses, treatment, dates of service, and provider names) were potentially compromised in the Data Breach.

Plaintiff Ruth Kidder

28. Plaintiff Kidder is an adult individual and a natural person of New Hampshire, residing in Merrimack County, where she intends to stay.

29. Plaintiff Kidder provided her Private Information to Harvard Pilgrim as a condition of receiving health-related services. Upon information and belief, Plaintiff Kidder's Private Information was stored and maintained by Defendant Harvard Pilgrim.

30. Plaintiff Kidder received a notice letter from Defendant Harvard Pilgrim dated June 15, 2023 informing her of the Data Breach and the exposure of her Private Information.

31. The notice letter informed Plaintiff Kidder that her name, address, Social Security number phone number, date of birth, health insurance information, and clinical information (medical history, diagnoses, treatment, dates of service, and provider names) were potentially compromised in the Data Breach.

Plaintiff Daniel Neal

32. Plaintiff Neal is an adult individual and a natural person of Tennessee, residing in Sevier County, where he intends to stay.

33. Plaintiff Neal provided his and his minor children's Private Information to Harvard Pilgrim as a condition of receiving health-related services. Upon information and belief, Plaintiff Neal's and his minor children's Private Information was stored and maintained by Defendant Harvard Pilgrim.

34. Plaintiff Neal received notice letters from Defendant Harvard Pilgrim dated June 15, 2023 informing him of the Data Breach and the exposure of his and his minor children's Private Information.

35. The notice letters informed Plaintiff Neal that his and his minor children's names, address, Social Security numbers, phone number, dates of birth, health insurance information, and clinical information (medical history, diagnoses, treatment, dates of service, and provider names) were potentially compromised in the Data Breach.

Plaintiff Danielle Olson

36. Plaintiff Olson is an adult individual and a natural person of Illinois, residing in DuPage County, where she intends to stay.

37. Plaintiff Olson provided her Private Information Harvard Pilgrim as a condition of receiving health-related services. Upon information and belief, Plaintiff Olson's Private Information was stored and maintained by Defendant Harvard Pilgrim.

38. Plaintiff Olson received a notice letter from her employer, Griffin, notifying her of the Data Breach and the exposure of her Private Information.

39. The notice letter informed Plaintiff Olson that her name, address, Social Security number phone number, date of birth, health insurance information, and clinical information were potentially compromised in the Data Breach.

Plaintiff Girard Patterson

40. Plaintiff Patterson is an adult individual and a natural person of Massachusetts, residing in Plymouth County, where he intends to stay.

41. Plaintiff Patterson provided his Private Information to Harvard Pilgrim as a condition of receiving health-related services. Upon information and belief, Plaintiff Patterson's Private Information was stored and maintained by Defendant Harvard Pilgrim.

42. Plaintiff Patterson received a notice letter from Defendant Harvard Pilgrim dated June 15, 2023 informing him of the Data Breach and the exposure of his Private Information.

43. The notice letter informed Plaintiff Patterson that his name, address, Social Security number phone number, date of birth, health insurance information, and clinical information (medical history, diagnoses, treatment, dates of service, and provider names) were potentially compromised in the Data Breach.

Plaintiff Tanya Peckham

44. Plaintiff Peckham is an adult individual and a natural person of Massachusetts, residing in Norfolk County, where she intends to stay.

45. Plaintiff Peckham provided her Private Information to Harvard Pilgrim as a condition of receiving health-related services. Upon information and belief, Plaintiff Peckham's Private Information was stored and maintained by Defendant Harvard Pilgrim.

46. Plaintiff Peckham received a notice letter from Defendant Harvard Pilgrim dated June 15, 2023 informing her of the Data Breach and the exposure of her Private Information.

47. The notice letter informed Plaintiff Peckham that her name, address, Social Security number phone number, date of birth, health insurance information, and clinical information (medical history, diagnoses, treatment, dates of service, and provider names) were potentially compromised in the Data Breach.

Plaintiff Margaret Donovan

48. Plaintiff Donovan is an adult individual and a citizen of Massachusetts.

49. Plaintiff Donovan provided her Private Information to Harvard Pilgrim as a condition of receiving health-related services. Upon information and belief, Plaintiff Donovan's Private Information was stored and maintained by Defendant Harvard Pilgrim.

50. Plaintiff Donovan received a notice letter from Defendant Harvard Pilgrim on or about June 15, 2023 informing her of the Data Breach and the exposure of her Private Information.

51. The notice letter informed Plaintiff Donovan that her name, address, Social Security number phone number, date of birth, health insurance information, and clinical information (medical history, diagnoses, treatment, dates of service, and provider names) were potentially compromised in the Data Breach.

Plaintiff Angela Rountree

52. Plaintiff Rountree is an adult individual and a natural person of New Hampshire, residing in Hillsborough County, where she intends to stay.

53. Plaintiff Rountree provided her Private Information to Harvard Pilgrim as a condition of receiving health-related services. Upon information and belief, Plaintiff Rountree's Private Information was stored and maintained by Defendant Harvard Pilgrim.

54. Plaintiff Rountree received a notice letter from Defendant Harvard Pilgrim informing her of the Data Breach and the exposure of her Private Information.

55. The notice letter informed Plaintiff Rountree that her Personal Information was potentially compromised in the Data Breach.

Plaintiff Tracie Wilson

56. Plaintiff Wilson is an adult individual and a natural person of New Hampshire, residing in Merrimack County, where she intends to stay.

57. Plaintiff Wilson provided her Private Information to Harvard Pilgrim as a condition of receiving health-related services. Upon information and belief, Plaintiff Wilson's Private Information was stored and maintained by Defendant Harvard Pilgrim.

58. Plaintiff Wilson received a notice letter from Defendant Harvard Pilgrim dated June 15, 2023 informing her of the Data Breach and the exposure of her Private Information.

59. The notice letter informed Plaintiff Wilson that her name, address, Social Security number phone number, date of birth, health insurance information, and clinical information (medical history, diagnoses, treatment, dates of service, and provider names) were potentially compromised in the Data Breach.

Defendants

60. Defendant Harvard Pilgrim Health Care, Inc. is a Massachusetts corporation, with its principal place of business at 1 Wellness Way, Canton, MA 02021.

61. Defendant, Point32Health, Inc. is a Massachusetts corporation, with its principal place of business at 1 Wellness Way, Canton, MA 02021. Point32Health, Inc. is the parent company of Harvard Pilgrim Health Care, Inc. and HPHC Insurance Company, Inc.

JURISDICTION AND VENUE

62. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Minimal diversity is established because some Plaintiffs and many members of the class are citizens of states different than that of Defendants.

63. This Court has personal jurisdiction over Defendants because Defendants maintain their principal places of business and headquarters in this District and conduct substantial business in this District.

64. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendants conduct substantial business in this District.

FACTUAL ALLEGATIONS

A. Defendants Collected and Stored the Private Information of Plaintiffs and Class Members

65. Point32Health is a healthcare company offering a broad range of health plans and tools for navigating healthcare and well-being. Point32Health is comprised of a family of companies, including Harvard Pilgrim.[5]

66. Founded nearly 50 years ago, Harvard Pilgrim is a subsidiary and brand of Point32Health providing health benefit plans, programs, and services to more than 1.1 million members in Massachusetts, New Hampshire, Maine, and beyond. [6]

67. Upon information and belief, Defendants received and maintained the Private Information of members, such as individuals' names, addresses, dates of birth, member identification numbers, date of health plan coverage, and/or employer names. These records are stored on Defendants' computer systems.

68. Because of the highly sensitive and personal nature of the information Defendants acquire and store, Defendants knew or reasonably should have known that they stored protected Private Information and must comply with healthcare industry standards related to data security and all federal and state laws protecting customers' and members' Private Information and provide adequate notice to customers if their PII or PHI is disclosed without proper authorization.

69. When Defendants collect this sensitive information, they promise to use reasonable measures to safeguard the Private Information from theft and misuse.

70. Defendants acquired, collected, and stored, and represented that they maintained reasonable security over Plaintiffs' and Class Members' Private Information.

71. By obtaining, collecting, receiving, and/or storing Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew, or should have

[5] https://www.point32health.org/about-us/our-family-of-companies/ (last accessed April 19,2024).
[6] *Id.*

known, that they were thereafter responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

72. Upon information and belief, Defendants promised to only share Plaintiffs' and Class Members' Private Information in limited circumstances, none of which include sharing such information with hackers.

73. Upon information and belief, Defendants represented to their members in written contracts, marketing materials, and otherwise that they would properly protect all Private Information it obtained. Upon information and belief, Defendants knew or reasonably should have known that such representations would be passed on to their clients' health plan members, including Plaintiffs and Class Members.

74. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

75. Upon information and belief, Plaintiffs and Class Members relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

76. Defendants could have prevented or mitigated the effects of the Data Breach by better securing their networks, properly encrypting their data, or better selecting and supervising their information technology partners.

77. Defendants' negligence in safeguarding Plaintiffs' and Class Members' Private Information was exacerbated by repeated warnings and alerts directed to protecting and securing

sensitive data, as evidenced by the trending data breach attacks in recent years. From 2017 to 2022, the damages from identity theft reached over $8 trillion dollars.[7]

78. The healthcare industry in particular has experienced a large number of high-profile cyberattacks even in just the short period preceding the filing of this Complaint, and cyberattacks, generally, have become increasingly more common. According to the HIPAA Journal, more healthcare data breaches were reported in 2023 than in any other year, and likewise, more records were breached in 2023 than any other year.[8] In 2023, there were 725 data breaches that resulted in 133 million records being exposed, stolen, or otherwise impermissibly disclosed, compared to 2022 where 51.9 million records were breached.[9]

79. In the context of data breaches, healthcare is "by far the most affected industry sector."[10] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[11] And according to the cybersecurity firm Mimecast, in one year 90%, of healthcare organizations experienced cyberattacks. [12]

80. Despite the prevalence of public announcements of data breaches and data security compromises making it readily apparent to anyone, including Defendants, in possession of sensitive and valuable personally identifiable information that it was not a matter of if they would be susceptible to a security incident which might result in a data breach, but when. Defendants

---

[7] https://www.juniperresearch.com/press/cybercrime-to-cost-global-business-over-8-trn.
[8] https://www.hipaajournal.com/healthcare-data-breach-statistics/.
[9] *Id.*
[10] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.
[11] *See id.*
[12] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

failed to take appropriate steps to protect Plaintiffs' and Class Members' Private Information from being compromised.

81. Defendants failed to properly select their information security partners.

82. Defendants failed to ensure the proper monitoring and logging of the ingress and egress of network traffic.

83. Defendants failed to ensure the proper monitoring and logging of file access and modifications.

84. Defendants failed to ensure the proper training of their employees and their technology partners' employees as to cybersecurity best practices.

85. Defendants failed to ensure fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

86. Defendants failed to timely and accurately disclose that Plaintiffs' and Class Members' Private Information had been improperly acquired or accessed.

87. Defendants knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured Private Information.

88. Defendants failed to provide adequate supervision and oversight of the Private Information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Private Information of Plaintiffs and Class Members, misuse the PHI/PII and potentially disclose it to others without consent.

89. Upon information and belief, Defendants failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

90. Upon information and belief, Defendants failed to ensure the proper encryption of Plaintiffs' and Class Members' Private Information and monitor user behavior and activity to identify possible threats.

B. The Data Breach

91. On or about May 24 of 2023, Defendants notified the public ("Notice of Data Breach" or "Notice") that their customers' data had been compromised in a Data Breach.

a. Harvard Pilgrim informed its members of the following:

> On April 17, 2023, Harvard Pilgrim discovered a cybersecurity ransomware incident that impacted systems that support Harvard Pilgrim Health Care Commercial and Medicare Advantage Stride℠ plans (HMO)/(HMO-POS). We are working with third-party cybersecurity experts to conduct a thorough investigation into this incident and remediate the situation. [13]

The letter further states:

> We take the privacy and security of the data entrusted to us seriously. We are continuing our active investigation and conducting extensive system reviews and analysis before we can resume our normal business operations. Unfortunately, the investigation identified signs that data was copied and taken from our Harvard Pilgrim systems from March 28, 2023, to April 17, 2023. We want to assure you that we are taking this incident extremely seriously, and we deeply regret any inconvenience this incident may cause.
>
> We determined that the files at issue may contain the following types of personal information and/or protected health information: names, physical addresses, phone numbers, dates of birth, health insurance account information, Social Security numbers, provider taxpayer identification numbers, and clinical information (e.g., medical history, diagnoses, treatment, dates of service, and provider names). [14]

b. Point32Health informed its members of the following:

> On April 17, Point32Health identified a cybersecurity ransomware incident that impacted systems we use to service members, accounts, brokers and providers. This is impacting systems that support Harvard Pilgrim Health Care commercial and Medicare Advantage Stride℠ plans (HMO)/(HMO-POS). Currently Tufts Health Plan, Tufts Medicare

[13] https://www.harvardpilgrim.org/data-security-incident/?_ga=2.131363663.1154609995.1685042380-1735340693.1685042380.
[14] Id.

> Preferred, Tufts Health Public Plans and CarePartners of Connecticut systems remain accessible. [15]
>
> The letter further states:
>
> Unfortunately, the investigation identified signs that data was copied and taken from our Harvard Pilgrim Health Care ("Harvard Pilgrim") systems between March 28, 2023, and April 17, 2023. We determined that the files at issue may contain personal information and/or protected health information for current and former subscribers and dependents, and current contracted providers.[16]

92. Upon information and belief, each Notice of Data Breach was drafted and publicized under the direction of both Defendants.

93. Although the Data Breach began on March 28, 2023, it was not until April 17, 2023—twenty days later—that Defendants first became aware of suspicious activity on their network.

94. Plaintiffs' and Class Members' Private Information was access, exfiltrated, and stolen in the Breach.

95. Plaintiffs' and Class Members' Private Information was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

96. While Defendants claim to have become aware of the Breach by April 17, 2023, Defendants did not begin notifying some victims of the Data Breach until May or June of 2023,—as long as two months later.

97. Time is of the essence when highly sensitive Private Information is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired Private Information of Plaintiffs and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiffs and Class Members are now subject to the present and continuing risk of fraud, identity

[15] https://www.point32health.org/systemupdate/.
[16] Id.

theft, and misuse resulting from the possible publication of their Private Information onto the Dark Web. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing sensitive personal information.

98. Following the Breach and recognizing that each Class Member is now subject to the present and continuing risk of identity theft and fraud, Defendants advised impacted individuals to "remain vigilant, monitor, and review their financial and account statements and explanations of benefits, and report any unusual activity to the institution that issued the record and to law enforcement."[17]

99. Defendants largely put the burden on Plaintiffs and Class Members to take measures to protect themselves.

100. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[18]

101. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week; [19] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable

[17] https://www.point32health.org/systemupdate/.
[18] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed Oct. 21, 2022); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data,* https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last accessed Aug. 2, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.).
[19] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019).

income.'" [20] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

102. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

103. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' Private Information with the intent of engaging in misuse of the Private Information, including marketing and selling Plaintiffs' and Class Members' Private Information.

104. Defendants also offered credit monitoring services to some Class Members for a period of 24 months. Such measures, however, are insufficient to protect Plaintiffs and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiffs and Class Members seek a sum of money sufficient to provide Plaintiffs and Class Members identity theft protection services for their respective lifetimes.

105. Defendants had and continue to have obligations created by HIPAA, reasonable industry standards, common law, state statutory law, and its own assurances and representations to keep Plaintiffs' and Class Members' Private Information confidential and to protect such Private Information from unauthorized access.

[20] *Id.*

106. Defendants' Breach Notice letter, as well as its website notice, both omit the size and scope of the breach. Defendants have demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

107. Plaintiffs and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular ransomware used, and what steps are being taken, if any, to secure their Private Information and financial information going forward. Plaintiffs and Class Members are left to speculate as to the full impact of the Data Breach and how exactly Defendants intend to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

108. Plaintiffs' and Class Members' Private Information and financial information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed Private Information and financial information for targeted marketing without the approval of Plaintiffs and/or Class Members. Either way, unauthorized individuals can now easily access the Private Information and/or financial information of Plaintiffs and Class Members.

C. Defendants Had Ample Notice that the Data Breach Could Take Place.

109. Defendants' negligence or reckless or knowing disregard of their obligations to safeguard the Private Information of Plaintiffs and the Class Members is evinced by the repeated warnings and alerts of which Defendants reasonably should have been aware concerning the need to protect and secure Plaintiffs' Private Information, especially in light of the substantial increase in cyberattacks and data breaches in the healthcare and health insurance industries in the years preceding the date of this attack.

110. Specifically, as early as July 30, 2021, the U.S. Department of Health and Human Services ("HHS") issued an alert about potential threats to healthcare organizations from cyber-

attacks.[21] Referring to it as a "nightmare," HHS recommended that healthcare organizations ensure they review the list of recommended mitigations in the Alert and promptly apply them to impacted systems in their infrastructure.[22]

111. On August 25, 2021, the HHS Cybersecurity Program published another Alert entitled "Indicators of Compromise Associated with Hive Ransomware."[23] The Alert was also widely circulated and reported on by the media after its release.[24] HHS in particular noted that unauthorized parties had targeted entities in the healthcare and public health sector. The Alert, issued in conjunction with the FBI, described recommendations to detect, avoid, and recover from unauthorized party intrusions.[25] The Alert contains a list of specific, technical indicators that would immediately advise companies such as Defendants that a system has been compromised, recognizing that awareness of these indicators could allow for detection during an attack and can help contain or minimize its impact.[26]

---

[21] *See* HHS Cybersecurity Program H3: Section Alert (July 30, 2021), HiveNightmare/SeriousSAM Potential HPH Impact, https://www.hhs.gov/sites/default/files/sector-alert-hive-nightmare-serious-sam-tlpwhite.pdf (last accessed April 5, 2024).

[22] *See* HHS Cybersecurity Program H3: Section Alert (July 30, 2021), HiveNightmare/SeriousSAM Potential HPH Impact, www.hhs.gov/sites/default/files/sector-alert-hive-nightmare-serious-sam-tlpwhite.pdf (last accessed April 5, 2024).

[23] *See* HHS Cybersecurity Program HC3: Alert (August 25, 2021), www.hhs.gov/sites/default/files/iocs-associated-with-hive-ransomware-alert.pdf (last accessed April 5, 2024).

[24] *See, e.g.,* FBI Flash TLP White: Indicators of Compromise Associated with Hive Ransomware – August 25, 2021, American Hospital Association (8/25/21), www.aha.org/fbi-tlp-alert/2021-08-25-fbi-flash-tlp-white-indicators-compromise-associated-hive-ransomware (last accessed April 5, 2024).

[25] *See* FBI Flash TLP:White dated August 25, 2021, https://www.aha.org/fbi-tlp-alert/2021-08-25-fbi-flash-tlp-white-indicators-compromise-associated-hive-ransomware (last accessed April 5, 2024).

[26] *See* HHS Cybersecurity Program HC3: Analyst Note (April 18, 2022), www.hhs.gov/sites/default/files/hive-ransomware-analyst-note-tlpwhite.pdf (last accessed April 8, 2024).

112. The FBI Flash Alert also contained recommended mitigations that companies such as Defendants should immediately undertake:

a. Back-up critical data offline.

b. Ensure copies of critical data are in the cloud or on an external hard drive or storage device.

c. Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the data resides.

d. Use two-factor authentication with strong passwords, including for remote access services.

e. Monitor cyber threat reporting regarding the publication of compromised VPN login credentials and change passwords/settings if applicable. Keep computers, devices, and applications patched and up-to-date.

f. Install and regularly update anti-virus or anti-malware software on all hosts.[27]

It appears based on the amount of time this attack went unnoticed that Defendants failed and refused to adopt these recommended mitigations.

113. As another HHS Analysis points out:

> When defending against Hive or any other ransomware variant, there are standard practices that should be followed. *Prevention is always the optimal approach*. This includes but is not limited to the following: Use two-factor authentication with strong passwords – this is especially applicable for remote access services such as RDP and VPNs.
>
> a. Sufficiently backing up data, especially the most critical, sensitive and operationally necessary data is very important. We recommend the 3-2-1 Rule for the most important data: Back this data up in three different locations, on at least two different forms of media, with one of them stored offline.
>
> b. Continuous monitoring is critical, and should be supported by a constant input of threat data (open source and possibly proprietary as well)

[27] *Id.* at 7-8. The August Alert also contains links to additional resources to prevent, protect against, and respond to ransomware events.

> c. An active vulnerability management program must be comprehensive in scope and timely in implementation of the latest software updates. It should apply to traditional information technology infrastructure as well as any medical devices or equipment that is network-connected.
>
> d. Endpoint security should be comprehensive in scope and updated with the latest signatures/updates aggressively.[28]

114. Despite numerous attempts on the part of the federal government to inform healthcare and insurance organizations like Defendants of the threat posed by such attacks, and despite Defendants' enjoying more than a year to prepare and prevent such an attack based on the recommendations provided in these and other notices, Defendants were negligent, reckless, or intentionally tortious in their failure to take steps to adequately prepare for this wholly foreseeable event. It appears that Defendants did not have multi-factor authentication in place with the requirement of strong passwords; did not sufficiently arrange for back up data to be stored in a safe location that could be quickly brought back on line; did not engage in continuous system monitoring or otherwise set up a system that would identify and prevent access from an increase in unauthorized account access, did not acquire or implement an active vulnerability management program or comprehensive endpoint security measures that would have detected the fact that hackers had gained access to Defendants' computer systems for three weeks without being detected.

115. This unauthorized access, disclosure, and exfiltration remains fully unremedied and Harvard Pilgrim's systems are still adversely impacted. Defendants failed to provide notice to affected consumers in the most expedient time possible and without unreasonable delay, nor did it provide complete and accurate notice.

---

[28] HHS Cybersecurity Program HC3: Analyst Note, *supra* (emphasis added).

D. Defendants Violated Their Statutory and Regulatory Obligations to Protect Plaintiffs' Data.

116. Defendants knew, or reasonably should have known, the importance of safeguarding the Private Information entrusted to them and of the foreseeable consequences of a breach of the security of their computer network. Defendants were on notice that they should have and could have prevented this attack by properly securing and encrypting the Private Information of Plaintiffs and the Class Members and taking the steps outlined above to prevent infiltration by methods such as phishing by, for example, using multi-factor authentication methods. Defendants could also have destroyed data of certain former enrollees that was no longer useful, especially outdated data.

117. Thus, Defendants failed to take appropriate preventive actions to protect Plaintiffs' and Class Members' Private Information or records against release consistent with their obligations under both the laws set forth herein and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 C.F.R. § 160.102, and all HIPAA Administrative Simplification Regulations in effect on January 1, 2012, contained in Parts 160, 162, and 164 of Title 45 of the Code of Federal Regulations, and Part 2 of Title 42 of the Code of Federal Regulations, including, but not limited to, the following: (a) Developing and implementing security policies and procedures; and (b) Encrypting the information or records, and protecting against the release or use of the encryption key and passwords, or transmitting the information or records in a manner designed to provide equal or greater protections against improper disclosures.

118. Because Defendants are entities covered by HIPAA, they are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and 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, which establish national security standards and duties for Defendants' protection of Private Information maintained by them in electronic form.

119. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. "Electronic protected health information" is defined as "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

120. HIPAA's Security Rule requires Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (c) protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and (d) ensure compliance by their workforce.

121. HIPAA also requires Defendants to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(c), and also to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

122. The data breach at issue clearly meets the HIPAA Security Rule's definition of a "reasonably anticipated" threat or hazard to the security or integrity of Plaintiffs' and Class Members protected information. Similar cyberattacks have become so notorious that the FBI and U.S. Secret Service in 2019 issued a warning to potential targets like Defendants so that they

would become aware of a potential attack and prepare themselves to comply with their statutory and regulatory obligations. According to the cybersecurity firm Mimecast, 90% of healthcare organizations had experienced cyberattacks in the year of the FBI's report.[29]

123. The healthcare industry in particular experienced a large number of high-profile cyberattacks, placing Defendants on notice of the need to ensure their systems were not vulnerable to attacks like that suffered here. Cybersecurity breaches hit an all-time high in 2023, exposing a record amount of patient PHI. In 2023, 106 million individuals were affected by healthcare attacks, up from 44 million people in 2022.[30]

124. Due to the high-profile nature of these data breaches, Defendants either were or reasonably should have been on heightened notice of the threat of attacks occurring in the healthcare industry and, therefore, should have been on notice of their statutory and regulatory duties to protect against such attacks by diligently overseeing, preparing for, and immediately responding to such an attack. By the time of this cyberattack, Defendants should have been aware that ransomware attacks were on the upswing: "In 2022 [cyber-security firm Blackfog] recorded a total of 376 attacks, a 29% increase over 2021 and 34% increase from 2020. Key take aways from these overall numbers is that 89% of all attacks now involve data exfiltration, 9% more than in 2021. From a tactical point of view we also saw an increase in the use of PowerShell, now at

[29] *See* Mimecast Research: 90 Percent of Healthcare Organizations Hit with an Email-Borne Attack in the Past Year, Nasdaq (Mar. 10, 2020) https://www.nasdaq.com/press-release/mimecast-research:-90-percent-of-healthcare-organizations-hit-with-an-email-borne (last accessed April 19, 2024).

[30] *Healthcare cyberattacks have affected more than 100 million people in 2023*, December 18, 2023, https://www.chiefhealthcareexecutive.com/view/health-data-cyberattacks-have-affected-more-than-100-million-people-in-2023 (last accessed April 24, 2024).

87% of all attacks, a 7% increase from 2021 . . . . the Dark Web was used in 23% of all attacks, a dramatic increase from 5% in 2021."[31]

125. Despite the prevalence of public announcements alerting Defendants of the risks presented to Plaintiffs and Class Members, Defendants failed to take appropriate steps to comply with their statutory and regulatory duties to protect Plaintiffs' and Class Members' Private Information.

126. The attack on Defendants clearly establishes that they did not comply with HIPAA Rules. This attack resulted from a combination of insufficiencies that demonstrate Defendants failed to implement safeguards mandated by HIPAA regulations, including, but not limited to, the following:

a. Failing to ensure the confidentiality and integrity of electronic PHI that Defendants create, receive, maintain, and transmit, in violation of 45 C.F.R. section 164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights such as by the use of multi factor authentication, in violation of 45 C.F.R. section 164.312(a)(1);

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. section 164.308(a)(1);

d. Failing to identify and respond to suspected or known security incidents and mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. section 164.308(a)(6)(ii);

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

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

[31] BlackFog, 2022 Ransomware Attack Report, January 20, 2023, www.blackfog.com/2022-ransomware-attack-report/ (last accessed April 9, 2024)

g. Failing to ensure compliance with HIPAA security standard rules by its workforce by providing for adequate comprehensive training rather than simply using training software to test staff by imitating phishing emails, in violation of 45 C.F.R. section 164.306(a)(4);
h. Impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons, in violation of 45 C.F.R. section 164.502, *et seq.*;

i. Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI beyond simply using training software to test staff by imitating phishing emails, in violation of 45 C.F.R. sections 164.530(b) and 164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. section 164.530(c).

127. Defendants also violated their duties under the Federal Trade Commission Act, 15 U.S.C. § 45 et seq. ("FTC Act"). The FTC pursuant to that Act and regulations promulgated thereunder has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" that violates the FTC Act.

128. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[32] To that end, the FTC has issued numerous guidelines identifying data-security practices that businesses, such as Defendants, should employ to protect against the unlawful exfiltration of Private Information.

[32] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), bit.ly/3uSoYWF (last accessed April 9, 2024).

129. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[33] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

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

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

130. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

131. The FTC recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[34]

132. 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[33] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), bit.ly/3u9mzre (last accessed April 9, 2024).
[34] *See Start with Security*, *supra*.

133. These FTC enforcement actions include actions against healthcare providers and partners like Defendants. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

134. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to member Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

135. The applicable FTC rules, regulations, and guidelines obligated businesses like Defendants to protect Private Information from unauthorized access or disclosure by unauthorized persons.

136. At all relevant times, Defendants were fully aware of their obligation to protect their enrollees' Private Information because they are sophisticated business entities in the business of maintaining and transmitting Private Information.

137. Defendants were also aware of the significant consequences of their failure to protect Private Information for the millions of enrollees who provided their Private Information to Defendants, and knew that this data, if hacked, would injure Plaintiffs and Class Members.

138. Defendants failed to comply with applicable FTC rules, regulations and guidelines, and industry standards concerning the protection and security of Private Information. As evidenced by the duration, scope, and nature of the Data Breach, among its many deficient practices, Defendants failed in, inter alia, the following respects:

a. Developing and employing adequate intrusion detection systems;

b. Engaging in regular reviews of audit logs and authentication records;

c. Developing and maintaining adequate data security systems to reduce the risk of data breaches and cyberattacks;

d. Ensuring the confidentiality and integrity of current and former subscribers' Private Information that Defendants receive and maintain;

e. Protecting against any reasonably anticipated threats or hazards to the security or integrity of their current and former subscribers' Private Information;

f. Implementing policies and procedures to prevent, detect, contain, and correct security violations;

g. Developing adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;

h. Implementing technical policies, procedures and safeguards for electronically stored information concerning Private Information that permit access for only those persons or programs that have specifically been granted access; and

i. Other similar measures to protect the security and confidentiality of its current and former enrollees' Private Information.

139. Had Defendants implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. Defendants could have prevented or detected the Data Breach prior to the hackers accessing Defendants' systems and extracting sensitive and personal information for three weeks; the amount and/or types of Private Information accessed by the hackers could have been avoided or greatly reduced; and Plaintiffs and Class Members would have been notified sooner, allowing them to promptly take protective and mitigating actions.

140. As established by these laws, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants also owed a duty to Plaintiffs and Class Members to provide reasonable security in compliance with industry standards and state and

federal requirements, and to ensure that their computer systems, networks, and protocols adequately protected this Private Information and were not exposed to infiltration. This also included a duty to Plaintiffs and Class Members to design, maintain, and test their computer systems to ensure that the Private Information in their possession was adequately secured and protected; to create and implement reasonable data security practices and procedures to protect the Private Information in their possession and avoid access to their systems through processes such as phishing, including adequately training employees and others who accessed information within their systems on how to adequately protect Private Information; to avoid permitting such infiltration such as by use of multi-factor authentication; to implement processes that would detect a breach of their data security systems in a timely manner and to act upon data security warnings and alerts in a timely fashion; to promptly and fully disclose if their computer systems and data security practices were inadequate to safeguard individuals' Private Information from theft or exfiltration; and to disclose in a timely and accurate manner when data breaches or cyber-attacks occurred.

141. Defendants owed these duties to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendants affirmatively chose to design their systems with inadequate user authentication, security protocols and privileges, and set up faulty patching and updating protocols and backup systems. These affirmative decisions resulted in unauthorized parties being able to execute this attack and exfiltrate the data in question, to the injury and detriment of Plaintiffs and Class Members. By taking affirmative acts inconsistent with these obligations that left Defendants' computer systems vulnerable to such an attack, Defendants disclosed and permitted the disclosure of Private Information of Plaintiffs and Class Members to unauthorized third parties. Through such actions

or inactions, Defendants failed to preserve the confidentiality of Private Information they were duty-bound to protect.

142. Defendants represented that they cared about data security and the safeguarding of subscribers' Private Information, and they represented that they would keep secure and confidential the Private Information belonging to their current and former enrollees.

143. Plaintiffs' and Class Members' Private Information was provided to Defendants in reasonable understanding of their promises and self-imposed obligations to keep Private Information confidential, and to secure the Private Information from unauthorized access by malevolent actors. Defendants failed to do so.

144. The length of the Data Breach, the period of time it went undetected, and the years of information impacted also demonstrates that Defendants failed to adequately safeguard Private Information by, *inter alia,* maintaining an adequate data security environment to reduce the risk of a data breach; periodically auditing their security systems to discover intrusions like the Data Breach; deleting outdated information to protect against unnecessary risks of exposure; and retaining outside vendors to periodically test their network, servers, systems and workstations.

145. Had Defendants undertaken the actions that federal and state law require, the Data Breach could have been prevented or the consequences of the Data Breach significantly reduced, as Defendants would have detected the Data Breach prior to the hackers extracting data from Defendants' networks, and Defendants' enrollees would have been notified of the Data Breach sooner, allowing them to take necessary protective or mitigating measures much earlier.

146. Indeed, following the Data Breach, Defendants effectively conceded that their security practices were still inadequate and ineffective. In the FAQ for the Notice made publicly available, they admitted that two months after the breach several of their systems were still

impacted or offline: "System limitations impacted coverage under Harvard Pilgrim Health Care Commercial and Medicare Advantage Stride℠ plans."[35]

E. Plaintiffs Suffered Harm as a Result of the Data Breach.

147. The Data Breach presents serious, present, continuing, and largely irredeemable harm for all affected.[36]

148. Plaintiffs and Class Members are members of health plans who use Defendants for delivering health services.

149. As a prerequisite of receiving treatment, Defendants requires its customers' health plan members—like Plaintiffs and Class Members—to disclose their Private Information.

150. When Defendants finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Defendants' Breach Notice sent to members fails to explain how the breach occurred (what security weakness was exploited), what exact data elements of each affected individual were compromised, who the Breach was perpetrated by, and the extent to which those data elements were compromised.

151. Because of the Data Breach, Defendants inflicted injuries upon Plaintiffs and Class Members. And yet, Defendants have done little to provide Plaintiffs and the Class Members with relief for the damages they suffered.

152. All Class Members were injured when Defendants caused their Private Information to be exfiltrated by cybercriminals.

---

[35] Harvard Pilgrim HealthCare, "Notice of Data Security Accident, Frequently Asked Questions," https://www.harvardpilgrim.org/public/notice-of-data-security-incident (last accessed on April 25, 2024).

[36] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers (last accessed on April 10, 2024).

Plaintiff Docanto's Experience

153. Plaintiff Docanto values her privacy and makes every effort to keep her personal information private.

154. Plaintiff Docanto only allowed Defendants to maintain, store, and use her Private Information because she believed that Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

155. When her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Docanto suffered injury from a loss of privacy.

156. Plaintiff Docanto has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals.

157. Plaintiff Docanto has received notifications and alerts in or about June 1, 2023 that her Private Information was on the dark web

158. Furthermore, Plaintiff Docanto has experienced a marked increase in spam calls and texts as a result of the Data Breach.

159. The Data Breach has also caused Plaintiff Docanto to suffer present, continuing and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

160. As a result of the actual harm she has suffered, and the present, continuing and increased risk of future harm, Plaintiff Docanto has frozen her credit with each of the major credit reporting companies.

161. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Docanto to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

162. The present, continuing and substantial risk of harm and loss of privacy have both caused Plaintiff Docanto to suffer stress, fear, and anxiety. Plaintiff Docanto constantly worries about her savings and her retirement and fears that when she gets paid her money will disappear as a result of the Data Breach.

163. Plaintiff Docanto has a continuing interest in ensuring that Plaintiff Docanto's Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Dyer's Experience

164. Plaintiff Dyer values his and his family's privacy and makes every effort to keep his and his family's personal information private.

165. Plaintiff Dyer only allowed Defendants to maintain, store, and use his and his minor children's Private Information because he believed that Defendants would use basic security measures to protect that Private Information, such as requiring passwords and multi-factor authentication to access databases storing his and his minor children's Private Information.

166. When his and his minor children's Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Dyer suffered injury from a loss of privacy.

167. Plaintiff Dyer has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals.

168. Plaintiff Dyer's Private Information has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of an unauthorized person opening a Bank of America account in his name, fraudulent applications for payday loans being applied for in his name, and a notification that his information may be on the dark web from multiple sources following the Data Breach. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Dyer's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

169. Furthermore, Plaintiff Dyer has experienced a marked increase in spam calls and spam text messages as a result of the Data Breach.

170. The Data Breach has also caused Plaintiff Dyer to suffer present, continuing and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

171. As a result of the actual harm he has suffered, and the present, continuing and increased risk of future harm, Plaintiff Dyer froze his credit, arranged for a family Life Lock plan to protect his and his minor children's Private Information.

172. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Dyer to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This

time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

173. The present, continuing and substantial risk of harm and loss of privacy have both caused Plaintiff Dyer to suffer stress, fear, and anxiety. Plaintiff Dyer also worries about how the Data Breach and loss of his minor children's information will affect their lives.

174. Plaintiff Dyer has a continuing interest in ensuring that his and his minor children's Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Elaine's Experience

175. Plaintiff Elaine values her privacy and makes every effort to keep her personal information private.

176. Plaintiff Elaine only allowed Defendants to maintain, store, and use her Private Information because she believed that Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

177. When her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Elaine suffered injury from a loss of privacy.

178. Plaintiff Elaine has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Elaine entrusted to Defendants. This information has inherent value that Plaintiff Elaine was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals.

179. Plaintiff Elaine's Private Information has already been stolen and misused as she has experienced incidents fraud and identity theft so far. She has received a hospital bill in her name from hospital that she does not attend and a visit that she did not undertake. She has also received

notifications from credit monitoring software that her name was being used to make credit inquiries. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Elaine's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

180. Furthermore, Plaintiff Elaine has experienced an uptick in spam calls and emails as a result of the Data Breach.

181. The Data Breach has also caused Plaintiff Elaine to suffer present, continuing and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

182. As a result of the actual harm she has suffered, and the present, continuing and increased risk of future harm, Plaintiff Elaine closed all of her credit cards and placed a fraud watch on her account. She spent $50 to set up her own credit monitoring with Experian as a result of the Data Breach and froze her credit.

183. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Elaine to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to prevent further fraudulent activity, speaking with Harvard Pilgrim and her doctor about the Breach, and placing extra security on her online financial accounts. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

184. The present, continuing and substantial risk of harm and loss of privacy have both caused Plaintiff Elaine to suffer stress, fear, anxiety, and emotional exhaustion.

185. Plaintiff Elaine has a continuing interest in ensuring that Plaintiff Elaine's Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Kidder's Experience

186. Plaintiff Kidder values her privacy and makes every effort to keep her personal information private.

187. Plaintiff Kidder only allowed Defendants to maintain, store, and use her Private Information because she believed that Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

188. When her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Kidder suffered injury from a loss of privacy.

189. Plaintiff Kidder has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff Kidder was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals.

190. Plaintiff Kidder learned that in or about July 2, 2023, access to her Comcast email had been compromised and an attempt was made to have her pay to have her control of this account restored. Plaintiff Kidder also discovered that in or around July 2, 2023, access to her Facebook account was compromised and Plaintiff Kidder lost access to the contents thereof.

191. Furthermore, Plaintiff Kidder has experienced a marked increase in spam calls and texts as a result of the Data Breach.

192. The Data Breach has also caused Plaintiff Kidder to suffer present, continuing, and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

193. As a result of the actual harm she has suffered, and the present, continuing, and increased risk of future harm, Plaintiff Kidder has filed reports with her bank, her local police, the FBI and the FTC.

194. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Kidder to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

195. The present, continuing, and substantial risk of harm and loss of privacy have both caused Plaintiff Kidder to suffer stress, fear, and anxiety. Plaintiff Kidder has lost sleep and constantly worries about her accounts as a result of the Data Breach.

196. Plaintiff Kidder has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Neal's Experience

197. Plaintiff Neal values his and his family's privacy and makes every effort to keep his and his family's personal information private.

198. Plaintiff Neal only allowed Defendants to maintain, store, and use his and his minor children's Private Information because he believed that Defendants would use basic security measures to protect his and his minor children's Private Information, such as requiring passwords

and multi-factor authentication to access databases storing his and his minor children's Private Information.

199. When his and his minor children's Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Neal and his minor children suffered injury from a loss of privacy.

200. Plaintiff Neal and his minor children have been further injured by the damages to and diminution in value of his and his minor children's Private Information—a form of intangible property that Plaintiff Neal entrusted to Defendants. This information has inherent value that Plaintiff Neal and his minor children were deprived of when his and his minor children's Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals.

201. Plaintiff Neal was the victim of attempted fraud and identity theft. In approximately January 2024, Plaintiff Neal was advised by his bank that someone, using his name and Social Security number, was attempting to open a bank account at another bank. Since Plaintiff Neal had informed his bank of the Data Breach, the bank was able to prevent the fraudulent use of Plaintiff Neal's information to open an account at another bank.

202. Plaintiff Neal has also received notifications of attempts to fraudulently make purchases on both his debit and credit cards.

203. Furthermore, Plaintiff Neal has experienced a marked increase in spam calls and texts as a result of the Data Breach.

204. The Data Breach has also caused Plaintiff Neal to suffer present, continuing, and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from his and his minor children's Private Information being placed in the hands of criminals.

205. As a result of the actual harm he and his minor children have suffered, and the present, continuing and increased risk of future harm, Plaintiff has closed or changed bank accounts, credit and debit cards.

206. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Neal to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

207. The present, continuing, and substantial risk of harm and loss of privacy have both caused Plaintiff Neal to suffer stress, fear, and anxiety. Plaintiff Neal fears losing his good credit, which he has worked hard to attain, and worries about how the Data Breach and loss of his minor children's information will affect their lives.

208. Plaintiff Neal has a continuing interest in ensuring that Plaintiff Neal's Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Olson's Experience

209. Plaintiff Olson values her privacy and makes every effort to keep her personal information private.

210. Plaintiff Olson only allowed Defendants to maintain, store, and use her Private Information because she believed that Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

211. When her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Olson suffered injury from a loss of privacy.

212. Plaintiff Olson has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Olson entrusted to Defendants. This information has inherent value that Plaintiff Olson was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals.

213. Plaintiff Olson's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft so far including a marked increase in spam calls. The actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Olson's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

214. The Data Breach has also caused Plaintiff Olson to suffer present, continuing, and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

215. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Olson to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

216. The present and substantial risk of present and continuing harm and loss of privacy have both caused Plaintiff Olson to suffer stress, fear, and anxiety, particularly because her minor son's information may also have been compromised in the breach.

217. Plaintiff Olson has a continuing interest in ensuring that Plaintiff Olson's Private Information, which, upon information and belief, remains backed up in Defendants' possession,

is protected, and safeguarded from future breaches.

Plaintiff Patterson's Experience

218. Plaintiff Patterson values his privacy and makes every effort to keep his personal information private.

219. Plaintiff Patterson only allowed Defendants to maintain, store, and use his Private Information because he believed that Defendants would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information.

220. When his Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Patterson suffered injury from a loss of privacy.

221. Plaintiff Patterson has been further injured by the damages to and diminution in value of his Private Information—a form of intangible property that Plaintiff Patterson entrusted to Defendants. This information has inherent value that Plaintiff Patterson was deprived of when his Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals.

222. Plaintiff Patterson's Private Information has already been stolen and misused as he has experienced incidents of fraud and identity theft so far in the form of having his credit card number compromised twice since the Data Breach, resulting in him having to request new cards. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Patterson's life as a whole, and specifically caused financial strain on him as a direct result of the Data Breach.

223. Furthermore, Plaintiff Patterson has experienced a marked increase in spam calls and spam emails requesting his personal information, receiving upwards of 30 emails daily as a result of the Data Breach.

224. The Data Breach has also caused Plaintiff Patterson to suffer present, continuing, and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals.

225. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Patterson to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. Plaintiff Patterson estimates he has spent at least one or two hours per week on such activities since learning of the Data Breach. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

226. The present, continuing, and substantial risk of harm and loss of privacy have both caused Plaintiff Patterson to suffer stress, fear, and anxiety.

227. Plaintiff Patterson has a continuing interest in ensuring that Plaintiff Patterson's Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Peckham's Experience

228. Plaintiff Peckham values her privacy and makes every effort to keep her personal information private.

229. Plaintiff Peckham only allowed Defendants to maintain, store, and use her Private Information because she believed that Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

230. When her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

231. Plaintiff Peckham has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Peckham entrusted to Defendant. This information has inherent value that Plaintiff Peckham was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals.

232. Plaintiff Peckham's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft so far in the form of unauthorized persons: opening a PayPal account in her name, placing credit inquiries for a home equity loan causing her credit score to drop from a 798 to a 614, and creating fraudulent charges on her credit and debit cards resulting in her having to cancel the same. Plaintiff also received a medical bill for a treatment that she did not receive in New Hampshire. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Peckham's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

233. Furthermore, Plaintiff Peckham has experienced a marked increase in spam calls and texts as a result of the Data Breach.

234. The Data Breach has also caused Plaintiff Peckham to suffer present, continuing and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

235. As a result of the actual harm she has suffered, and the present, continuing and increased risk of future harm, Plaintiff Peckham has suffered a decline in her credit score, seen an increase in interest rates offered to her because of the same.

236. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Peckham to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

237. The present, continuing, and substantial risk of harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety. Plaintiff Peckham has also suffered several panic attacks since learning of the Data Breach.

238. Plaintiff Peckham has a continuing interest in ensuring that Plaintiff Peckham's Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Donovan's Experience

239. Plaintiff Donovan values her privacy and makes every effort to keep her personal information private.

240. Plaintiff Donovan only allowed Defendants to maintain, store, and use her Private Information because she believed that Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

241. When her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Donovan suffered injury from a loss of privacy.

242. Plaintiff Donovan has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Donovan entrusted to Defendants. This information has inherent value that Plaintiff Donovan was deprived of when her

Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals.

243. As a result of the Data Breach, Plaintiff Donovan was forced to spend approximately a hundred hours, in total, checking her bank statements and, on many occasions, speaking with bank representatives in order to reverse unauthorized charges.

244. Further, as a result of the Data Breach, Plaintiff Donovan's credit score and credit limit were lowered. Further, she was disqualified from promotional rates and had to borrow funds to meet her needs. Having sold her house, she was unable to buy a new one due to the credit score which was lowered as a result of the Data Breach. Plaintiff Donovan resorted to renting a dwelling as a result.

245. Also, as a result of the Data Breach, Plaintiff Donovan has suffered from a significant increase in spam communications, including phone calls, texts and emails.

246. The Data Breach has also caused Plaintiff Donovan to suffer present, continuing and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

247. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Donovan to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

248. The present, continuing, and substantial risk of harm and loss of privacy have both caused Plaintiff Donovan to suffer stress, fear, and anxiety.

249. Plaintiff Donovan has a continuing interest in ensuring that Plaintiff Donovan's Private Information, which, upon information and belief, remains backed up in Defendants'

possession, is protected, and safeguarded from future breaches.

Plaintiff Rountree's Experience

250. Plaintiff Rountree values her privacy and makes every effort to keep her personal information private.

251. Plaintiff Rountree only allowed Defendants to maintain, store, and use her Private Information because she believed that Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information.

252. When her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Rountree suffered injury from a loss of privacy.

253. Plaintiff Rountree has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendants. This information has inherent value that Plaintiff Rountree was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals.

254. Plaintiff Rountree's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft so far. Plaintiff Rountree's financial information was used to make unauthorized purchases for Facebook advertising. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Rountree's life as a whole, and specifically caused financial strain on her as a direct result of the Data Breach.

255. Furthermore, Plaintiff Rountree and her husband have experienced an onslaught of spam calls and text messages, including calls related to a business loan and credit checks.

256. The Data Breach has also caused Plaintiff Rountree to suffer present, continuing, and impending injury arising from the present and substantially increased risk of future fraud, identity

theft, and misuse resulting from her Private Information being placed in the hands of criminals.

257. As a result of the actual harm she has suffered, and the present, continuing, and increased risk of future harm, Plaintiff Rountree is now required to contact her bank for every business-related check for approval to ensure no further fraudulent activity occurs.

258. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Rountree to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. She and her husband have spent more than 75 hours attending information sessions, calling banks and credit agencies to mitigate impacts from the loss of their Private Information. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

259. The present, continuing and substantial risk of harm and loss of privacy have both caused Plaintiff Rountree to suffer stress, fear, and anxiety. She and her husband have experienced an increased amount of stress around paying their bills for their business.

260. Plaintiff Rountree has a continuing interest in ensuring that Plaintiff Rountree's Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Wilson's Experience

261. Plaintiff Wilson values her privacy and makes every effort to keep her personal information private.

262. Plaintiff Wilson only allowed Defendants to maintain, store, and use her Private Information because she believed that Defendants would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access

databases storing her Private Information.

263. When her Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Wilson suffered injury from a loss of privacy.

264. Plaintiff Wilson has been further injured by the damages to and diminution in value of her Private Information—a form of intangible property that Plaintiff Wilson entrusted to Defendants. This information has inherent value that Plaintiff Wilson was deprived of when her Private Information was placed on a publicly accessible database, exfiltrated by cybercriminals.

265. Plaintiff Wilson's Private Information has already been stolen and misused as she has experienced incidents of fraud and identity theft so far in the form of unauthorized persons attempting to change the information relating to her Visa card and attempting to charger her USAA checking account on two occasions requiring her to replace the cards for those accounts. Additionally, the credit monitoring provided by Harvard Pilgrim informed Plaintiff Wilson that her information was on the dark web. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff' Wilsons life as a whole, and specifically caused financial strain on him/her/them as a direct result of the Data Breach.

266. Furthermore, Plaintiff Wilson has experienced a marked increase in spam calls and text messages, including around five to six calls from Medicare on a daily basis and "click the link" texts attempting to lure her to provide personal information as a result of the Data Breach.

267. The Data Breach has also caused Plaintiff Wilson to suffer present, continuing, and impending injury arising from the present and substantially increased risk of future fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

268. As a result of the actual harm she has suffered, and the present, continuing, and increased risk of future harm, Plaintiff Wilson has incurred at least one late fee as a result of

changing her account information after her accounts were compromised.

269. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Wilson to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. Plaintiff Wilson estimates she has spent over 70 hours addressing the ramifications of this Data Breach. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

270. The present and substantial risk of present and continuing harm and loss of privacy have both caused Plaintiff Wilson to suffer stress, fear, and anxiety.

271. Plaintiff Wilson has a continuing interest in ensuring that Plaintiff Wilson's Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

272. Plaintiffs and Class Members entrusted their Private Information to Defendants. Thus, Plaintiffs had the reasonable expectation and understanding that Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents. After all, Plaintiffs would not have entrusted their Private Information to any entity that used Defendants' services had they known that Defendants would not take reasonable steps to safeguard their information.

273. Plaintiffs and Class Members suffered actual injury from having their Private Information compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their Private Information—a form of property that Defendants obtained

from Plaintiffs; (b) violation of their privacy rights; (c) the likely theft of their Private Information; (d) fraudulent activity resulting from the Breach; (e) nominal damages; (f) failure to receive the benefit of their bargains; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

274. As a result of the Data Breach, Plaintiffs and Class Members also suffered emotional distress because of the release of their Private Information—which they believed would be protected from unauthorized access and disclosure. Now, Plaintiffs suffer from anxiety about unauthorized parties viewing, selling, and/or using their Private Information for nefarious purposes like identity theft and fraud.

275. Plaintiffs and Class Members also suffer anxiety about unauthorized parties viewing, using, and/or publishing their information related to their medical records and prescriptions.

276. Because of the Data Breach, Plaintiffs and Class Members have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

F. The Value of the Private Information Demonstrates that Plaintiffs and Others Have Lost, Will Lose, or are at a Present and Continuing Risk of Losing Valuable Money or Property as a Result of this Data Breach.

277. It has been well established in both academic and popular discourse for more than a decade that Private Information is a valuable commodity[37] that makes it the frequent target of hackers. Plaintiffs and Class Members have lost or are reasonably certain to lose money or property because their data was permitted by Defendants to be improperly accessed or stolen. The

[37] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

ramifications of Defendants' failure to properly secure Plaintiffs' and Class Members' Private Information are thus material and severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes. Identity theft either has or is reasonably certain to happen to Plaintiffs and Class Members as a result of Defendants' acts and omissions.

278. Defendants either were or should have been aware that the Private Information they collect is highly sensitive and of significant value to those who would use it for wrongful purposes. As the FTC has reported, identity thieves can use this information to commit an array of crimes including identify theft, medical and financial fraud.[38] Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.

279. A robust cyber black market exists in which criminals post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web, to create fake insurance claims, purchase and resell medical equipment, or access prescriptions for illegal use or resale. Criminals often trade stolen Private Information on the "cyber black market" for years following a breach. For example, it is believed that certain Private Information compromised in the 2017 Experian data breach was being used three years later by identity thieves to apply for COVID-19-related benefits.[39] According to a 2017 Javelin strategy and research

[38] Federal Trade Commission, What To Know About Identity Theft, https://consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed April 10, 2024).
[39] Janelle Stecklein, *Director: 64,000-plus fraudulent unemployment claims 'mitigated'*, The Duncan Banner (June 24, 2020), https://www.duncanbanner.com/news/director-64-000-plus-fraudulent-unemployment-claims-mitigated/article_dc446671-73a6-5e8a-b732-bcedba72b458.html (last accessed April 10, 2023).

presentation, fraudulent activities using data stolen in data breaches between two and six years old had increased by nearly 400% over the previous 4 years.[40]

280. In this case, compromised personal credentials belonging to a Defendants' employee has been found on the dark web.

281. According to Experian, one of the three major credit bureaus, medical records can be worth up to $1,000 per person on the dark web, depending upon completeness.[41] Private Information can be sold at a price ranging from approximately $20 to $300.[42]

282. Medical identify theft can also result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences since if a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[43]

---

[40] *See*, Brian Stack, Here's How Much Your Personal Information is Selling for on the Dark Web
(2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed April 10, 2023).
[41] *Id.*
[42] www.privacyaffairs.com/dark-web-price-index-2021/
[43] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, (2/7/14), https://khn.org/news/rise-of-indentity-theft/ (last accessed April 11, 2024); *See also*, *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare (last accessed April 11, 2024).

283. The Ponemon Institute found that "health care identity theft victims spend nearly $13,500" to resolve complications and that victims often have to pay off the imposter's fraudulent medical bills.[44]

284. In another study by the Ponemon Institute in 2015, 31% of medical identity theft victims lost their healthcare coverage as a result of the incident, while 29% had to pay to restore their health coverage, and over half were unable to resolve the identity theft at all.[45]

285. Once Private Information is stolen, such as membership identification numbers or Social Security numbers, fraudulent use of that information and damage to victims may continue for years. According to the U.S. Government Accountability Office ("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."[46] The ramifications of Defendants' failure to protect Plaintiffs' and Class Members' Private Information and to advise them of all the relevant facts are not a temporary inconvenience but a long-lasting threat, because the fraudulent use of that information and the damage to victims may continue for years. Private Information have a long shelf-life because they contain different forms of personal information, some of which never

[44] Brian O'Connor, Healthcare Data Breach: What to Know About Them and What to Do After One, Experian (June 14, 2018), www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed April 11, 2024).
[45] Ponemon Institute, *Fifth Annual Study on Medical Identity Theft*, (February 2015), www.medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf (last accessed April 11, 2015).
[46] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, gao.gov/products/gao-07-737 (last accessed April 11, 2024).

changes over the course of a victim's life (and even after), such as Social Security Numbers and Dates of Birth, the information can be used in more ways than one, and it typically takes time, as it has in this case, for the extent of an information breach to be detected.

286. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[47]

287. Defendants' wrongful actions and/or inactions and the resulting Data Breach have placed Plaintiffs and the Class at an present, immediate, and continuing heightened risk of identity theft and identity fraud. There is also a high likelihood that significant identity fraud and/or identity theft affecting Class Members has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class Members' Private Information will exploit it at a later date or re-sell it to a criminal who will.

288. In response to the Data Breach, Harvard Pilgrim has established a dedicated call center for individuals to contact with questions or concerns and for potentially impacted individuals to enroll in complimentary credit monitoring and identity theft protection services. However, because there is no description provided as to the information or services Defendants provide, and because Defendants themselves cannot determine the extent of the damage or the

[47] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last accessed last accessed April 11, 2024).

risks caused by their negligent, reckless, or intentional acts or omissions, this response is inadequate to protect against the lifelong risk of harm imposed on Plaintiffs and Class Members by Defendants' failures.

289. Plaintiffs and Class Members have suffered present, continuing, and impending injury arising from the substantially present and continuing risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will not abate within a mere one to two years: the unauthorized access of Plaintiffs' and Class Members' Private Information, especially their Social Security numbers, puts Plaintiffs and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that Defendants have indicated they will offer victims of the Data Breach.

290. Plaintiffs retain an interest in ensuring there are no future data breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both themselves and similarly situated individuals whose Private Information was accessed in the Data Breach.

CLASS ACTION ALLEGATIONS

291. Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), seek certification of the following Nationwide Class and state subclasses (together the "Classes"):

> **Nationwide Class**
>
> All persons residing in the United States whose PII or PHI was impacted by the Data Breach—including all who were sent a notice of the Data Breach.
>
> **Massachusetts Subclass**
>
> All persons residing in the State of Massachusetts whose PII or PHI was compromised in the Data Breach, including all who were sent

a notice of the Data Breach (the "Massachusetts Subclass").

Maine Subclass

All persons residing in the State of Maine whose PII or PHI was compromised in the Data Breach, including all who were sent a notice of the Data Breach (the "Maine Subclass").

New Hampshire Subclass

All persons residing in the State of New Hampshire whose PII or PHI was compromised in the Data Breach, including all who were sent a notice of the Data Breach (the "New Hampshire Subclass").

Illinois Subclass

All persons residing in the State of Illinois whose PII or PHI was compromised in the Data Breach, including all who were sent a notice of the Data Breach (the "Illinois Subclass").

Tennessee Subclass

All persons residing in the State of Tennessee whose PII or PHI was compromised in the Data Breach, including all who were sent a notice of the Data Breach (the "Tennessee Subclass").

292. Excluded from the Classes are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendants or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendants' counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

293. Plaintiffs reserve the right to amend or modify the Class definitions as this case progresses.

294. Plaintiffs satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

295. Numerosity: The Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendants and obtainable by Plaintiffs only through the discovery process, reports indicate that over 2.8 million individuals comprise the Class and were affected by the Data Breach. The members of the Class will be identifiable through information and records in Defendants' possession, custody, and control.

296. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class Members. These common legal and factual questions include, but are not limited to:

a. Whether Defendants' data security and retention policies were unreasonable;

b. Whether Defendants failed to protect the confidential and highly sensitive information with which they were entrusted;

c. Whether Defendants owed a duty to Plaintiffs and Class Members to safeguard their Private Information;

d. Whether Defendants breached any legal duties in connection with the Data Breach;

e. Whether Defendants' conduct was intentional, reckless, willful, or negligent;

f. Whether an implied contract was created concerning the security of Plaintiffs' and Class Members' Private Information;

g. Whether Defendants breached that implied contract by failing to protect and keep secure Plaintiffs' and Class Members' Private Information and/or failing to timely and adequately notify Plaintiffs and Class Members of the Data Breach;

h. Whether Plaintiffs and Class Members suffered damages as a result of Defendants' conduct; and

i. Whether Plaintiffs and the Class are entitled to monetary damages, injunctive relief and/or other remedies and, if so, the nature of any such relief.

297. Typicality: All of Plaintiffs' claims are typical of the claims of the Class since Plaintiffs and all members of the Class had their Private Information compromised in the Data Breach. Plaintiffs and the members of the Class sustained damages as a result of Defendants' uniform wrongful conduct.

298. Adequacy: Plaintiffs are adequate representatives because their interests do not materially or irreconcilably conflict with the interests of the Class they seek to represent, they have retained counsel competent and highly experienced in complex class action litigation, and they intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Neither Plaintiffs nor their counsel have any interests that are materially antagonistic to the interests of other members of the Class.

299. Superiority: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. 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. Members of the Class can be readily identified and notified based on, *inter alia*, Defendants' records and databases.

300. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CAUSES OF ACTION

COUNT I – NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

301. Plaintiffs incorporate and reallege all factual allegations above as if fully set forth herein.

302. Defendants required Plaintiffs and Class Members to provide Defendants with Private Information in order to receive Defendants products and services.

303. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Defendants owed a duty of care to use reasonable means to secure and safeguard their computer system—and Plaintiffs' and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes so they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

304. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendants held vast amounts of Private Information, it was inevitable that unauthorized individuals would at some point try to access Defendants' databases of Private Information.

305. After all, Private Information is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiffs and Class Members. Thus, Defendants knew, or should have known, the importance

of exercising reasonable care in handling the Private Information entrusted to them.

306. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

307. Defendants' duty of care to use reasonable security measures arose because of the special relationship that existed between Defendants and Plaintiffs and Class Members, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

308. Defendants failed to take appropriate measures to protect the Private Information of Plaintiffs and the Class. Defendants are morally culpable, given the prominence of security breaches in the healthcare industry. Any purported safeguards that Defendants had in place were wholly inadequate.

309. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class Members' Private Information by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in the healthcare industry, and allowing unauthorized access to Plaintiffs' and the other Class Members' Private Information.

310. The failure of Defendants to comply with industry and federal regulations evinces Defendants negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information.

311. But for Defendants wrongful and negligent breach of their duties to Plaintiffs and the Class, Private Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' negligence was a direct and legal cause of the theft of the Private Information of Plaintiffs and the Class and all resulting damages.

312. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendants failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class Members' Private Information. Defendants knew or should have known that their systems and technologies for processing and securing the Private Information of Plaintiffs and the Class had security vulnerabilities.

313. As a result of this misconduct by Defendants, the PII, PHI, and other sensitive information of Plaintiffs and the Classes was compromised, placing them at a greater risk of identity theft and their Private Information being disclosed to third parties without the consent of Plaintiff and the Class.

314. As a direct and proximate result of Defendants negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information; (viii) future costs in terms of time, effort and money that will be expended

to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by Defendants data breach; (x) the value of the unauthorized access to their PII/PHI permitted by Defendants; and (xi) any nominal damages that may be awarded.

315. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses including nominal damages.

316. Defendants negligent conduct is ongoing, in that they still possess Plaintiffs' and Class Members' Private Information in an unsafe and insecure manner.

317. Plaintiffs and Class Members are entitled to injunctive relief requiring Defendants to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II – NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Nationwide Class)

318. Plaintiffs incorporate and reallege all factual allegations above as if fully set forth herein.

319. Defendants had duties arising under HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and the FTC Act to protect Plaintiffs' and Class Members' Private Information.

320. Defendants breached their duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following: (i) failing to adopt, implement, and

maintain adequate security measures to safeguard Class Members' Private Information; (ii) failing to adequately monitor the security of their networks and systems; (iii) allowing unauthorized access to Class Members' Private Information; (iv) failing to detect in a timely manner that Class Members' Private Information had been compromised; (v) failing to remove former employees' Private Information they were no longer required to retain pursuant to regulations; and (vi) failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

321. Defendants' violation of HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

322. Plaintiffs and Class Members are consumers within the class of persons that HIPAA, HITECH, and Section 5 of the FTC Act were intended to protect.

323. The harm that has occurred is the type of harm HIPAA, HITECH, and the FTC Act were intended to guard against.

324. The FTC has pursued enforcement actions against businesses and healthcare entities that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

325. Defendants breached their duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

326. Plaintiffs and Class Members were foreseeable victims of Defendants violations of HIPAA, HITECH, and the FTC Act. Defendants knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiffs' and Class

Members' Private Information would cause damage to Plaintiffs and the Class.

327. As a direct and proximate result of Defendants negligence per se, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by Defendants data breach; (x) the value of the unauthorized access to their PII/PHI permitted by Defendants; and (xi) any nominal damages that may be awarded.

328. As a direct and proximate result of Defendants negligence per se, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury, including, but not limited to anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

329. Finally, as a direct and proximate result of Defendants negligence per se, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect

the Private Information in its continued possession.

COUNT III – BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

330. Plaintiffs incorporate and reallege all factual allegations above as if fully set forth herein.

331. Defendants required Plaintiffs and the Class to provide and entrust their PII/PHI and financial information as a condition of obtaining services from Defendants.

332. Plaintiffs and the Class paid money to Defendants in exchange for goods and services, as well as Defendants' promises to protect their protected health information and other Private Information from unauthorized disclosure.

333. Defendants promised to comply with HIPAA standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

334. Through its course of conduct, Defendants, Plaintiffs, and Class Members entered into implied contracts for Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PHI and PII and financial information.

335. Defendants solicited and invited Plaintiffs and Class Members to provide their PHI/PII and financial information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their PHI/PII and financial information to Defendants.

336. As a condition of being direct customers/members of Defendants, Plaintiffs and Class Members provided and entrusted their PHI/PII and financial information to Defendants. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class

Members if its data had been breached and compromised or stolen.

337. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide its PHI/PII and financial information to Defendants, in exchange for, amongst other things, the protection of its PHI/PII and financial information.

338. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

339. Defendants breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their PHI/PII and financial information and by failing to provide timely and accurate notice to them that their PHI/PII and financial information was compromised as a result of the Data Breach.

340. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to comply with its promise to abide by HIPAA.

341. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendants created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1).

342. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

343. Defendants further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

344. Defendants' failures to meet these promises constitute breaches of the implied contracts.

345. Furthermore, the failure to meet its confidentiality and privacy obligations resulted in Defendants providing goods and services to Plaintiffs and Class Members that were of a diminished value.

346. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) (a) present, ongoing, and continuing threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

347. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the present and continuing risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

348. Plaintiffs and Class Members are entitled to compensatory, nominal, and consequential damages suffered as a result of the Data Breach.

349. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit and identity monitoring to all Class Members.

COUNT IV – BAILMENT
(On Behalf of Plaintiffs and the Nationwide Class)

350. Plaintiffs incorporate and reallege all factual allegations above as if fully set forth herein.

351. Defendants required Plaintiffs and the Class to provide and entrust their Private Information as a condition of obtaining services from Defendants.

352. In delivering their Private Information, Plaintiffs and Class Members intended and understood that their Private Information would be adequately safeguarded and protected.

353. Defendants accepted Plaintiffs' and Class Members' Private Information.

354. By accepting possession of Plaintiffs' and Class Members' Private Information, Defendants understood and accepted that Plaintiffs and the Class expected their Private Information to be adequately safeguarded and protected. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

355. During the bailment (or deposit), Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care, diligence, and prudence in protecting their Private Information.

356. Defendants breached their duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class Members' Private Information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and Class Members' Private Information.

357. Defendants further breached their duty to safeguard Plaintiffs' and Class Members' Private Information by failing to timely notify them that their Private Information had been compromised as a result of the Data Breach.

358. Defendants failed to return, purge, or delete the Private Information belonging to Plaintiffs and Class Members at the conclusion of the bailment (or deposit) and within the time

limits allowed by law.

359. As a direct and proximate result of Defendants' breach of their duties, Plaintiffs and the Class suffered consequential damages that were reasonably foreseeable to Defendants, and Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

COUNT V – VIOLATION OF THE MASSACHUSETTS CONSUMER PROTECTION ACT
Mass. Gen. Laws Ann. Ch. 93a, §§ 1, et seq.

(On Behalf of Plaintiffs Docanto, Patterson, and Peckham, Donovan and the Massachusetts Subclass)

360. Plaintiffs Docanto, Patterson, Peckham and Donovan (for the purposes of this count, "Plaintiffs") reallege and incorporate by reference the factual allegations contained in the aforementioned paragraphs.

361. This claim is brought individually under the laws of Massachusetts and on behalf of all other natural persons whose Private Information was compromised.

362. Defendants, Plaintiffs and Massachusetts Subclass Members are "persons" as meant by Mass. Gen. Laws. Ann. Ch. 93A, § 1(a).

363. Defendants operate in "trade or commerce" as meant by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

364. Defendants advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

365. Defendants engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including by:

a. Failing to implement and maintain reasonable security and privacy measures to protect Massachusetts Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Massachusetts Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Massachusetts Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Massachusetts Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;

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

g. Omitting, suppressing, and concealing the material fact that it did not comply with

common law and statutory duties pertaining to the security and privacy of Massachusetts Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

366. Defendants' acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that Defendants solely held the true facts about its inadequate security for Private Information, which Massachusetts Subclass Members could not independently discover.

367. Defendants' representations and omissions were material because Defendants knew the representations and omissions were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Private Information.

368. Defendants acted intentionally, knowingly, and maliciously to violate Massachusetts law and recklessly disregarded Plaintiffs' and Massachusetts Subclass Members' rights.

369. Plaintiffs and Massachusetts Subclass Members justifiably relied on the above-mentioned misrepresentations.

370. Plaintiffs and Massachusetts Subclass Members would not have engaged in business with Defendants nor provided Defendants with their Private Information but for Defendants' misrepresentations regarding its protection of that Private Information.

371. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiffs and Massachusetts Subclass Members have suffered and will continue to suffer actual damages, ascertainable losses of money or property, and monetary and nonmonetary damages, as described herein, including but not limited to: fraud and identity theft; time and

expenses related to monitoring their financial and other accounts for fraudulent activity; an increased, continuing risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendants products and services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

372. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the Plaintiffs affected by the Data Breach.

373. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiffs and Massachusetts Subclass Members that they could not reasonably avoid.

374. Plaintiffs and Massachusetts Subclass Members seek all monetary and non-monetary relief allowed by law under Mass. Gen. Laws. Ann. Ch. 93A, § 1(a), including actual damages or statutory damages (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs; and any other relief that the Court deems appropriate.

COUNT VII – VIOLATION OF ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
815 ILCS 505/1
(On Behalf of Plaintiff Danielle Olson and the Illinois Subclass)

375. Plaintiff Danielle Olson (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the factual allegations contained in the aforementioned paragraphs.

376. Plaintiff brings this claim on behalf of themselves and the Illinois Subclass.

377. Defendants, Plaintiff, and Illinois Subclass Members are "persons" as meant by 815 ILCS 505/1(c).

378. Defendants engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of 815 ILCS 505 et seq, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff' sand Illinois Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Illinois Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164.

379. Defendants' acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

380. Defendants' representations and omissions were material because Defendants knew the representations and omissions were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Private Information.

381. Defendants acted intentionally, knowingly, and maliciously to violate Illinois law and recklessly disregarded Plaintiff's and Illinois Subclass Members' rights.

382. Plaintiff and Illinois Subclass Members justifiably relied on the above-mentioned misrepresentations.

383. Plaintiff and Illinois Subclass Members would not have engaged in business with Defendants nor provided Defendants with their Private Information but for Defendants' misrepresentations regarding its protection of that Private Information.

384. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer actual damages, ascertainable losses of money or property, and monetary and nonmonetary damages, as described herein, including but not limited to: fraud and identity theft; time and expenses related

to monitoring their financial and other accounts for fraudulent activity; a present and continuing risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendants products and services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

385. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the plaintiffs affected by the Data Breach.

386. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiff and Illinois Subclass Members that they could not reasonably avoid.

387. Plaintiff and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs; and any other relief that the Court deems appropriate.

COUNT VIII – VIOLATION OF MAINE UNFAIR TRADE PRACTICES ACT
Me. Rev. Stat. tit. 5, §§ 205-A- §214
(On Behalf of Plaintiffs Justin Dyer, Svea Elaine, and the Maine Subclass)

388. Plaintiffs Justin Dyer and Svea Elaine (for the purposes of this count, "Plaintiffs") reallege and incorporate by reference the factual allegations contained in the aforementioned paragraphs.

389. Plaintiffs bring this claim on behalf of themselves and the Maine Subclass.

390. Defendants, Plaintiffs and Maine Subclass Members are "persons" as meant by Me. Rev. Stat. tit. 5, §206.

391. Defendants operate in "trade or commerce" as meant by Me. Rev. Stat. tit. 5, §206.

392. Defendants engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of Me. Rev. Stat. tit. 5, §§ 205-A-

§214, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Maine Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Maine Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Maine Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Maine Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Maine Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164.

393. Defendants' representations and omissions were material because Defendants knew the representations and omissions were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Private Information.

394. Defendants acted intentionally, knowingly, and maliciously to violate Maine law and recklessly disregarded Plaintiffs' and Maine Subclass Members' rights.

395. Plaintiffs and Maine Subclass Members justifiably relied on the above-mentioned misrepresentations.

396. Plaintiffs and Maine Subclass Members would not have engaged in business with Defendants nor provided Defendants with their Private Information but for Defendants' misrepresentations regarding its protection of that Private Information.

397. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiffs and Maine Subclass Members have suffered and will continue to suffer actual damages, ascertainable losses of money or property, and monetary and nonmonetary damages, as described herein, including but not limited to: fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; a present and continuing risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendants products and services; loss of the value of access to their Private Information; and the

value of identity protection services made necessary by the Data Breach.

398. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the Plaintiffs affected by the Data Breach.

399. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiffs and Maine Subclass Members that they could not reasonably avoid.

400. Plaintiffs and Maine Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs; and any other relief that the Court deems appropriate.

COUNT IX – VIOLATION OF NEW HAMPSHIRE CHAPTER 358-A FOR REGULATION OF BUSINESS PRACTICES FOR CONSUMER PROTECTION
N.H. Rev. Stat. Ann. §§ 358–A:1 to 358–A:13
(On Behalf of Plaintiff Kidder, Plaintiff Rountree, Plaintiff Wilson, and the New Hampshire Subclass)

401. Plaintiffs Kidder, Wilson, and Rountree (for the purposes of this count, "Plaintiffs") reallege and incorporate by reference the factual allegations contained in the aforementioned paragraphs.

402. Plaintiffs bring this claim on behalf of themselves and the New Hampshire Subclass.

403. Defendants, Plaintiffs and New Hampshire Subclass Members are "persons" as meant by N.H. Rev. Stat. Ann. §§ 358–A:1.

404. Defendants operate in "trade or commerce" as meant by N.H. Rev. Stat. Ann. §§ 358–A:1.

405. Defendants engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.H. Rev. Stat. Ann. §§ 358–A:1 to 358–A:13, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and New Hampshire Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New Hampshire Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New Hampshire Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and New Hampshire Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and New Hampshire Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164.

406. Defendants' acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

407. Defendants' representations and omissions were material because Defendants knew the representations and omissions were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Private Information.

408. Defendants acted intentionally, knowingly, and maliciously to violate New Hampshire law and recklessly disregarded Plaintiffs' and New Hampshire Subclass Members' rights.

409. Plaintiffs and New Hampshire Subclass Members justifiably relied on the above-mentioned misrepresentations.

410. Plaintiffs and New Hampshire Subclass Members would not have engaged in business with Defendants nor provided Defendants with their Private Information but for Defendants' misrepresentations regarding its protection of that Private Information.

411. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiffs and New Hampshire Subclass Members have suffered and will continue to suffer actual damages, ascertainable losses of money or property, and monetary and nonmonetary

damages, as described herein, including but not limited to: fraud and identity theft; time and expenses related to monitoring their financial and other accounts for fraudulent activity; a present and continuing risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendants products and services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

412. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the Plaintiffs affected by the Data Breach.

413. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiffs and New Hampshire Subclass Members that they could not reasonably avoid.

414. Plaintiffs and New Hampshire Consumer Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs; and any other relief that the Court deems appropriate.

COUNT X – VIOLATION OF TENESSEE CONSUMER PROTECTION ACT OF 1977

Tenn. Code Ann. § 47-18-103 to § 47–18–135
(On Behalf of Plaintiff Daniel Neal and the Tennessee Subclass)

415. Plaintiff Daniel Neal (for the purposes of this count, "Plaintiff") realleges and incorporates by reference the factual allegations contained in the aforementioned paragraphs.

416. Plaintiff brings this claim on behalf of himself and the Tennessee Subclass.

417. Defendants, Plaintiff and Tennessee Subclass Members are "persons" as meant by Tenn. Code Ann. § 47-18-103(18).

418. Defendants operate in "trade or commerce" as meant by Tenn. Code Ann. § 47-18-103(24).

419. Defendants engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of Tenn. Code Ann. § 47-18-103 to § 47–18–135, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Tennessee Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Tennessee Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Tennessee Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Tennessee Subclass Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Tennessee Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164.

420. Defendants' representations and omissions were material because Defendants knew the representations and omissions were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Private Information.

421. Defendants acted intentionally, knowingly, and maliciously to violate Tennessee law and recklessly disregarded Plaintiff's and Tennessee Subclass Members' rights.

422. Plaintiff and Tennessee Subclass Members justifiably relied on the above-mentioned misrepresentations.

423. Plaintiff and Tennessee Subclass Members would not have engaged in business with Defendants nor provided Defendants with their Private Information but for Defendants' misrepresentations regarding its protection of that Private Information.

424. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and Tennessee Subclass Members have suffered and will continue to suffer actual damages, ascertainable losses of money or property, and monetary and nonmonetary damages, as described herein, including but not limited to: fraud and identity theft; time and

expenses related to monitoring their financial and other accounts for fraudulent activity; a present and continuing risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendants products and services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

425. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the Plaintiff and Tennessee Subclass Members affected by the Data Breach.

426. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiff and Tennessee Subclass Members that they could not reasonably avoid.

427. Plaintiff and Tennessee Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs; and any other relief that the Court deems appropriate.

COUNT XI – INTRUSION UPON SECLUSION
(On Behalf of Plaintiffs and the Nationwide Class)

428. Plaintiffs incorporate and reallege all factual allegations above as if fully set forth herein.

429. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information that Defendants possessed and/or continue to possess.

430. By failing to keep Plaintiffs' and Class Members' Personal and Medical Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, Defendants invaded Plaintiffs' and Class Members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing or permitting the publication of private facts about Plaintiffs and Class Members, which is highly offensive to a reasonable person.

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

432. Defendants invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by misusing and/or disclosing or permitting the disclosure of their private information without their informed, voluntary, affirmative, and clear consent.

433. As a proximate result of such misuse and disclosures, Plaintiffs' and Class Members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Defendants' conduct amounted to a serious invasion of Plaintiffs' and Class Members' protected privacy interests.

434. In failing to protect Plaintiffs' and Class Members' Private Information, and in misusing and/or disclosing or permitting the disclosure of their Private Information, Defendants have acted with malice and oppression and in conscious disregard of Plaintiffs' and the Class Members' rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing their own economic, corporate, and legal interests above the privacy interests of over 2.8 million enrollees. Plaintiffs, therefore, seek an award of damages, including punitive damages, on behalf of Plaintiffs and the Class.

COUNT XII – UNJUST ENRICHMENT
(By Plaintiffs on behalf of the Nationwide Class)

435. Plaintiffs incorporate and reallege all factual allegations above as if fully set forth

herein.

436. This Claim is pleaded in the alternative to Count III above.

437. Plaintiffs and the Class have an interest, both equitable and legal, in their Private Information that was collected and maintained by Defendants.

438. Defendants were benefitted by the conferral upon them of Plaintiffs' and Class Members' Private Information and by their ability to retain and use that information. Defendants understood that they were in fact so benefitted.

439. Defendants also understood and appreciated that Plaintiffs' and Class Members' Private Information was private and confidential and its value depended upon Defendants' maintaining the privacy and confidentiality of that information.

440. But for Defendants' representations, both explicit and implied, that they would maintain the privacy and confidentiality of this Private Information, Plaintiffs and Class Members would not have provided or authorized their Private Information to be provided to Defendants, and Defendants would have been deprived of the competitive and economic advantages they enjoyed by falsely representing that their data-security safeguards met reasonable standards, or by omitting material facts to the contrary. These competitive and economic advantages include, without limitation, wrongfully gaining enrollees, gaining the reputational advantages conferred upon them by Plaintiffs and Class Members' enrollment, monetary savings resulting from Defendants' failure to reasonably upgrade and maintain data technology infrastructures, and their realization of excessive profits as a result thereof.

441. As a result of Defendants' wrongful conduct as alleged herein (including, among other things, their deception of Plaintiffs, members of the Class, and the public relating to the nature and scope of the Data Breach; their failure to employ adequate data security measures; their

continued maintenance and use of the Private Information belonging to Plaintiffs and Class Members without having adequate data security measures; and other conduct resulting in the theft of that Private Information as referenced above), Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class.

442. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion.

443. Under the common law doctrine of unjust enrichment, it is inequitable for Defendants to be permitted to retain the benefits they received, and are still receiving, without justification, from Plaintiffs and the Class in an unfair and unconscionable manner. Defendants' retention of such benefits under circumstances make it inequitable to do so, and thus constitutes unjust enrichment.

444. The benefit conferred upon, received, and enjoyed by Defendants was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendants to retain the benefit.

445. Defendants are therefore liable to Plaintiffs and the Class for restitution in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including specifically the value to Defendants of the Private Information that was accessed and exfiltrated in the Data Breach and the profits Defendants received from the monies they saved from their failure to reasonably upgrade and maintain their data technology infrastructures.

COUNT XIII – DECLARATORY JUDGMENT
(By Plaintiffs on behalf of the Nationwide Class)

446. Plaintiffs incorporate and reallege all factual allegations above as if fully set forth

herein.

447. This count is brought on behalf of all Class Members.

448. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described herein.

449. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' Private Information, and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information. Defendants have admitted that their data security measures remain inadequate as many key systems remain offline.

450. Plaintiffs and the Class continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

451. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following: (a) Defendants owe a legal duty to secure employees' Private Information, and to timely notify impacted individuals of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes, and (b) Defendants continue to breach this legal duty by failing to employ reasonable measures to secure Private Information in its possession.

a. Order Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendants explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. prohibit Defendants from engaging in the wrongful and unlawful acts alleged herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete and purge the Private Information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

v. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants systems on a periodic basis;

vi. prohibiting Defendants from maintaining Plaintiffs' and Class Members' Private Information on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Defendants to segment data by creating firewalls and access controls so that, if one area of Defendants network is compromised, hackers cannot gain access to other portions of Defendants systems;

viii. requiring Defendants to conduct regular database scanning and securing checks;

ix. requiring Defendants to monitor ingress and egress of all network traffic;

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xi. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendants to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendants networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Defendants to meaningfully educate all Class Members about the threats that it faces because of the loss of its confidential personal

identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

452. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at, or implicating, Defendants. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

453. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

454. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose confidential information would be further compromised.

COUNT XIV – BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(By Plaintiffs on behalf of the Nationwide Class)

455. Plaintiffs incorporate and reallege all factual allegations above as if fully set forth herein.

456. Defendants entered into a contract to provide services to Plaintiffs' respective medical providers, employers, and/or insurance companies. Upon information and belief, this contract is virtually identical to the contracts entered into between Defendants and their other

medical provider and insurance customers around the country whose patients were also affected by the Data Breach.

457. These contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their confidential medical information that Defendants agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

458. Defendants knew that if they were to breach these contracts with its customers, the customers' patients, including Plaintiffs and the Class, would be harmed by, among other harms, fraudulent transactions.

459. Defendants breached their contracts with the medical providers and/or insurance entities affected by this Data Breach when they failed to use reasonable data security measures that could have prevented the Data Breach.

460. As foreseen, Plaintiffs and the Class were harmed by Defendants' failure to use reasonable security measures to store patient information, including but not limited to the risk of harm through the loss of their Private Information.

461. Accordingly, Plaintiffs and the Class are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

COUNT XV – BREACH OF FIDUCIARY DUTY
(By Plaintiffs on behalf of the Nationwide Class)

462. Plaintiffs incorporate and reallege all factual allegations above as if fully set forth herein.

463. A relationship existed between Plaintiffs, the Class Members, and Defendants, which arose from Defendants' acceptance of Plaintiffs' and the Class Members' Private Information and Defendants' representations of its commitment to protect said Private Information.

464. In providing their Private Information to Defendants, Plaintiffs and Class Members justifiably placed a special confidence in Defendants to act in good faith and with due regard for the interests of Plaintiffs and Class Members to safeguard and keep confidential that Private Information.

465. Defendants accepted the special confidence Plaintiffs and Class Members placed in them, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiff's personal information as included in the Data Breach notification letter.

466. In light of the special relationship between Defendants, Plaintiffs, and Class Members, whereby Defendants became guardians of Plaintiffs' and Class Members' Private Information, Defendants created a fiduciary duty by their undertaking the guardianship of the Private Information, to act primarily for the benefit of their customers, including Plaintiffs and Class Members, for the safeguarding of Plaintiffs' and Class Members' Private Information.

467. Defendants have fiduciary duties to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their customer relationships, in particular, to keep secure the Private Information of their customers.

468. Defendants breached their fiduciary duties to Plaintiffs and Class Members by failing to protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

469. Defendants breached their fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs and Class Members' Private Information.

470. As a direct and proximate result of Defendants breaches of its fiduciary duties, Plaintiffs and Class Members have suffered or will suffer concrete injury, including, but not limited to: (a) actual identity theft; (b) the loss of the opportunity to determine how and when their Private Information is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the present and continued risk to their Private Information, which remains in Defendants possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in its continued possession and ensure that it retains vendors who adequately protect Private Information; (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, and repair the impact of the Private Information compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (h) nominal damages.

471. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully request the following relief:

A. An Order certifying this action as a class action and appointing Plaintiffs as Class Representatives;

B. A mandatory injunction directing Defendants to adequately safeguard the Private Information of Plaintiffs and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete and purge the Private Information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

v. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants' systems on a

periodic basis;

vi. prohibiting Defendants from maintaining Plaintiffs' and Class Members' Private Information on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Defendants to segment data by creating firewalls and access controls so that, if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

viii. requiring Defendants to conduct regular database scanning and securing checks;

ix. requiring Defendants to monitor ingress and egress of all network traffic;

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xi. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendants to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendants' networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Defendants to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that Defendants provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information;

E. An award of damages, including actual, statutory, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiffs and the Class leave to amend this Complaint to conform to the evidence produced at trial;

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury for any and all issues in this action so triable as of right.

Dated: April 26, 2024

Respectfully Submitted,

/s/ James Pizzirusso
James Pizzirusso*
HAUSFELD LLP
888 16th St. NW Suite 300
Washington, DC 20006
T: (202) 540-7200
jpizzirusso@hausfeld.com

/s/ *John Yanchunis*
John A. Yanchunis*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, Florida 33602
T: (813) 223-5505
F: (813) 223-5402
jyanchunis@forthepeople.com

Interim Co-Lead Counsel
for the Class

****Admitted Pro Hac Vice***

CERTIFICATE OF SERVICE

I, James J. Pizzirusso, hereby certify that on April 26, 2024, I caused a copy of the foregoing Consolidated Class Action Complaint to be filed electronically with the Clerk of the Court via the Court's CM/ECF electronic filing system, which will send a notification to all counsel of record.

/s/ James J. Pizzirusso
James J. Pizzirusso

ClassAction.org
