UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
SOUTHERN DIVISION

IN RE AACOM DATA BREACH LITIGATION	Case No. 8:25-cv-01239-TJS **CONSOLIDATED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Ted Christensen, Marina Girgis, Nicolas Sikaczowski, and Emily Scott (hereinafter "Plaintiffs"), by and through their attorneys, individually and on behalf of all others similarly situated, bring this Consolidated Class Action Complaint against Defendant American Association of Colleges of Osteopathic Medicine d/b/a AACOM ("AACOM" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to their own actions, counsels' investigations, and facts of public record.

NATURE OF ACTION

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

2. Defendant is a professional association focused on osteopathic medicine.[1] Defendant also "provides centralized services including data collection and analysis and operation of the online application service for students applying to US osteopathic medical schools."[2]

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about its current and former consumers (e.g., applicants to US osteopathic medical schools). But Defendant

[1] *About Us*, AACOM, https://www.aacom.org/about-us (last visited June 2, 2025).
[2] *Id*.

lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

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

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

6. Plaintiffs are Data Breach victims, having each received breach notices. Plaintiffs bring this class action on behalf of themselves, and all others harmed by Defendant's misconduct.

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

PARTIES

8. Plaintiff Ted Christensen is a natural person and citizen of the United States, residing in Saratoga Springs, Connecticut, where he intends to remain.

9. Plaintiff Marina Girgis is a natural person and citizen of the United States, residing in Fort Lee, New Jersey, where she intends to remain.

10. Plaintiff Nicolas Sikaczowski is a natural person and citizen of the United States, residing in Biddeford, Maine, where he intends to remain.

11. Plaintiff Emily Scott is a natural person and citizen of the United States, residing in Pittsburg, Pennsylvania, where she intends to remain.

12. Defendant, American Association of Colleges of Osteopathic Medicine d/b/a AACOM, is a nonstock corporation incorporated in Illinois and with its principal place of business at 7700 Old Georgetown Road, Suite 250, Bethesda, Maryland 20814 (Montgomery County).

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiffs and Defendant are citizens of different states. And there are more than 100 putative Class Members.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2), because a substantial part of the events or omissions giving rise to the claims occurred in Montgomery County, Maryland. Montgomery County lies within the Southern Division of the United States District Court for the District of Maryland pursuant to 28 U.S.C. § 100. Accordingly, this action is properly filed in the Southern Division of this Court.

FACTUAL BACKGROUND

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

15. Defendant is a professional association focused on osteopathic medicine.[3] Defendant also "provides centralized services including data collection and analysis and operation of the online application service for students applying to US osteopathic medical schools."[4]

16. As part of its business, Defendant receives and maintains the PII/PHI of thousands of its current and former consumers (e.g., applicants to US osteopathic medical schools).

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

[3] *About Us*, AACOM, https://www.aacom.org/about-us (last visited June 2, 2025).
[4] *Id*.

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

19. Defendant recognizes these duties, declaring in its "Privacy Policy" that:

a. "To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we strive to maintain physical, electronic, and administrative safeguards to secure the information we collect online."[5]

b. "This includes the use of the Secure Sockets Layer (SSL) for processing purchases and donations securely[.]"[6]

Defendant's Data Breach

20. On September 26, 2024, Defendant was hacked in the Data Breach.[7]

21. Worryingly, Defendant already admitted that "AACOM discovered unusual activity associated with an employee email account" and that "certain emails / attachments may have been accessed or acquired without authorization."[8]

22. The following types of PII/PHI were compromised in the Data Breach: names, Social Security numbers; and medical information.[9]

23. In total, Defendant injured at least 67,804 persons—via the exposure of their PII/PHI—in the Data Breach.[10] Upon information and belief, these 67,804 persons include its current and former consumers.

---

[5] *Privacy Policy*, AACOM (Dec. 2, 2024) https://www.aacom.org/home/Policies/privacy-policy.
[6] *Id*.
[7] *Data Breach Notification*, MAINE ATTY GEN (April 8, 2025) https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/61f2428d-b058-48da-b831-b0ea7543ac0f.html (last visited June 2, 2025).
[8] *Id*.
[9] *Id*.; *see also Data Breach Security Reports*, TEXAS ATTY GEN (April 10, 2025) https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (listing the types of exposed information as "Social Security Number Information; Medical Information").
[10] *Data Breach Notifications*, MAINE ATTY GEN (April 8, 2025) https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/61f2428d-b058-48da-b831-b0ea7543ac0f.html (last visited June 2, 2025).

24. And yet, Defendant waited until April 8, 2025, before it began notifying the class—a ***full 194 days*** after the Data Breach was discovered.[11]

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

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

a. "[W]e recommend that you remain vigilant by reviewing your account statements and credit reports closely."[12]

b. "[O]btain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft."[13]

27. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused widespread injury and monetary damages.

28. Since the Data Breach, Defendant claims that it "took steps to further secure its email environment and conducted a comprehensive investigation."[14] But such simple declarations are insufficient to ensure that Plaintiffs' and Class Members' PII/PHI will be protected from additional exposure in a subsequent data breach.

29. Further, the Notice of Data Breach shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when.

---

[11] *Id*.
[12] *Id*.
[13] *Id*.
[14] *Id*.

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

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

32. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[15]

33. Thus, on information and belief, Plaintiffs and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiff Ted Christensen's Experience and Injuries

34. Plaintiff Christensen applied to Osteopathic medical school through Defendant's website, which required him to provide his PII/PHI to Defendant.

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

36. As a result, Plaintiff Christensen was injured by Defendant's Data Breach.

37. Plaintiff Christensen is very careful about the privacy and security of his PII/PHI. He does not knowingly transmit his PII/PHI over the internet in an unsafe manner. He is careful to store any documents containing his PII/PHI in a secure location.

38. Plaintiff Christensen provided his PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Christensen's PII/PHI

[15] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back (last visited June 2, 2025).

and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

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

40. Plaintiff Christensen reasonably expected and understood that Defendant would take industry standard precautions to protect, maintain, and safeguard individuals' PII/PHI from unauthorized users or disclosure, and would timely notify individuals if any security incidents involving their PII/PHI arose. Plaintiff Christensen would not have provided his PII/PHI to Defendant had he known that Defendant would not take reasonable steps to safeguard it.

41. Plaintiff Christensen received a Notice Letter, dated April 8, 2025.

42. Thus, upon information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

43. Defendant's Data Breach compromised Plaintiff Christensen's name and Social Security number.

44. Plaintiff Christensen has spent—and will continue to spend—significant time and effort researching the Data Breach and monitoring his credit and financial accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its Breach Notice. ,

45. Plaintiff Christensen fears for his personal financial security and worries about what information was exposed in the Data Breach.

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

47. Plaintiff Christensen suffered actual injury from the exposure and theft of his PII.

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

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

50. As a result of the Data Breach, Plaintiff Christensen anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

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

Plaintiff Marina Girgis' Experience and Injuries

52. Plaintiff Marina Girgis applied to Osteopathic medical school through Defendant's website in or around the early 2010s, which required her to provide her PII/PHI to Defendant.

53. Thus, Defendant obtained and maintained Plaintiff Girgis' PII/PHI.

54. As a result, Plaintiff Girgis was injured by Defendant's Data Breach.

55. Plaintiff Girgis is very careful about the privacy and security of her PII/PHI. She does not knowingly transmit her PII/PHI over the internet in an unsafe manner. She is careful to store any documents containing her PII/PHI in a secure location.

56. Plaintiff Girgis provided her PII/PHI to Defendant and trusted Defendant to use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Girgis' PII/PHI and has a

continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

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

58. Plaintiff Girgis reasonably expected and understood that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard individuals' PII/PHI from unauthorized users or disclosure, and would timely notify individuals if any security incidents involving their PII/PHI arose. Plaintiff Girgis would not have provided her PII/PHI to Defendant had she known that Defendant would not take reasonable steps to safeguard it.

59. Plaintiff Girgis received a Notice Letter in April 2025.

60. Thus, upon information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

61. Defendant's Data Breach compromised Plaintiff Girgis' name and Social Security number.

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

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

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

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

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

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

68. As a result of the Data Breach, Plaintiff Girgis anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of her life.

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

Plaintiff Nicolas Sikaczowski's Experience and Injuries

70. Plaintiff Nicolas Sikaczowski provided his information to Defendant as a condition of becoming a member with Defendant.

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

72. As a result, Plaintiff Sikaczowski was injured by Defendant's Data Breach

73. Plaintiff Sikaczowski is very careful about sharing his sensitive PII/PHI. He does not knowingly transmit his PII/PHI over the internet in an unsafe manner. He is careful to store any documents containing his PII/PHI in a secure location.

74. Plaintiff Sikaczowski provided his PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Sikaczowski's

PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

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

76. Plaintiff Sikaczowski reasonably expected and understood that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard individuals' PII/PHI from unauthorized users or disclosure, and would timely notify individuals if any security incidents involving their PII/PHI arose. Plaintiff Sikaczowski would not have provided his PII/PHI to Defendant had he known that Defendant would not take reasonable steps to safeguard it.

77. Plaintiff Sikaczowski received a Notice Letter from Defendant dated April 8, 2025.

78. Thus, upon information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

79. Defendant's Data Breach compromised Plaintiff Sikaczowski's name and Social Security number.

80. As a result of the Data Breach, Plaintiff Sikaczowski made reasonable efforts to mitigate the impact of the Data Breach after receiving notice of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. After all, Defendant directed Plaintiff to take those steps in its breach notice. In fact, following the Data Breach, Plaintiff has already been alerted to attempts at password changes on his online profiles which he did not initiate.

81. Because of the Data Breach, Plaintiff Sikaczowski has spent significant time and will continue to spend valuable hours for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

82. Plaintiff Sikaczowski fears for his personal financial security and worries about what information was exposed in the Data Breach.

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

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

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

86. Plaintiff Sikaczowski suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Sikaczowski's PII/PHI right in the hands of criminals. As a result of the Data Breach, Plaintiff Sikaczowski anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

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

Plaintiff Emily Scott's Experience and Injuries

88. Plaintiff Emily Scott provided her information to Defendant as a condition of becoming a member with Defendant.

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

90. As a result, Plaintiff Scott was injured by Defendant's Data Breach.

91. Plaintiff Scott is very careful about the privacy and security of her PII/PHI. She does not knowingly transmit her PII/PHI over the internet in an unsafe manner. She is careful to store any documents containing her PII/PHI in a secure location. Plaintiff Scott provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Scott's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

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

93. Plaintiff Scott reasonably expected and understood that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard individuals' PII/PHI from unauthorized users or disclosure, and would timely notify individuals if any security incidents involving their PII/PHI arose. Plaintiff Scott would not have provided her PII/PHI to Defendant had she known that Defendant would not take reasonable steps to safeguard it.

94. Plaintiff Scott received a Notice Letter from Defendant dated April 8, 2025.

95. Thus, upon information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

96. Defendant's Data Breach compromised Plaintiff Scott's name and Social Security number.

97. As a result of the Data Breach, Plaintiff Scott made reasonable efforts to mitigate the impact of the Data Breach after receiving notice of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud. After all, Defendant directed Plaintiff to take those steps in its Breach Notice. In fact, following the Data

Breach, Plaintiff Scott has already been alerted to attempts at password changes on her online profiles which she did not initiate.

98. Because of the Data Breach, Plaintiff Scott has spent significant time and will continue to spend valuable hours for the remainder of her life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

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

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

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

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

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

104. As a result of the Data Breach, Plaintiff Scott anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of her life.

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

105. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[16] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[17]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[18]

c. 89% of consumers stated that "I care about data privacy."[19]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[20]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[21]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[22]

---

[16] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited June 2, 2025).
[17] *Id*. at 3.
[18] *Id*.
[19] *Id*. at 9.
[20] *Id*.
[21] *Id*.
[22] *Id*. at 11.

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

106. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages, including, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an higher risk of suffering: loss of the opportunity to control how their PII/PHI is used; diminution in value of their PII/PHI; compromise and continuing publication of their PII/PHI; out-of-pocket costs from trying to prevent, detect, and recover from identity theft and fraud; lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of their stolen PII/PHI; and continued risk to their PII/PHI—which remains in Defendant's possession—and is thus at risk for future breaches so long as Defendant fails to take appropriate measures to protect the PII/PHI.

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

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

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

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

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

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

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

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

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

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

116. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[23]

---

[23] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

117. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[24]

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

Defendant Failed to Follow FTC Guidelines

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

119. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[25] The FTC declared that, *inter alia*, businesses must: protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

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

121. Furthermore, the FTC explains that companies must: not maintain information longer than is needed to authorize a transaction; limit access to sensitive data; require complex

[24] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

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

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 use reasonable security measures.

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

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

Defendant Failed to Follow Industry Standards

124. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

125. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

126. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST

Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

Defendant Violated HIPAA

128. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[26]

129. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI and PHI is properly maintained.[27]

130. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to: failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1); failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of

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

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

electronic PHI in violation of 45 C.F.R. § 164.306(a)(2); failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3); failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4); failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1); failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1); failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii); failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

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

CLASS ACTION ALLEGATIONS

132. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by AACOM in September 2024, including all those individuals who received notice of the breach.

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

134. Plaintiffs reserve the right to amend the class definition.

135. Certification of Plaintiffs claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

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

137. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least 67,804 members.

138. Typicality. Plaintiffs claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

139. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class Members' interests. And Plaintiffs have retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

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

a duty to use reasonable care in safeguarding Plaintiffs and the Class's PII/PHI; if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; if Defendant were negligent in maintaining, protecting, and securing PII/PHI; if Defendant breached contract promises to safeguard Plaintiffs and the Class's PII/PHI; if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it; if Defendant's Breach Notice was reasonable; if the Data Breach caused Plaintiffs and the Class injuries; what the proper damages measure is; and if Plaintiffs and the Class are entitled to damages, treble damages, and/or injunctive relief.

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

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

142. Plaintiffs incorporate by reference paragraphs 1 through 145 as if fully set forth herein.

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

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

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

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

147. Defendant owed—to Plaintiffs and Class Members—at least the following duties: exercise reasonable care in handling and using the PII/PHI in its care and custody; implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized; promptly detect attempts at unauthorized access; notify Plaintiffs and Class Members within a reasonable timeframe of any breach to the security of their PII/PHI.

148. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

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

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

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

152. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate IT systems and data security practices to safeguard Plaintiffs and Class Members' PII/PHI.

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

154. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

155. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiffs and Class Members' PHI.

156. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too,

Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

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

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

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

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

161. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs and Class Members' PII/PHI by: disclosing and providing access to this information to third parties and failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

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

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

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

165. As a direct and proximate cause of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, and emotional distress.

166. And, on information and belief, Plaintiffs PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

167. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On behalf of the Plaintiffs and the Class)

168. Plaintiffs incorporate by reference paragraphs 1 through 145 as if fully set forth herein.

169. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class members' PII/PHI.

170. Defendant breached its duties to Plaintiffs and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and Class members' PII/PHI.

171. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

172. The injuries to Plaintiffs and Class members resulting from the Data Breach were directly and indirectly caused by Defendant's violation of the statutes described herein.

173. Plaintiffs and Class members were within the class of persons the Federal Trade Commission Act intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

174. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class members, Plaintiffs and Class members would not have been injured.

175. The injuries and harms suffered by Plaintiffs and Class members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that Defendant's breach would cause Plaintiffs and Class members to experience the harms associated with the exposure of their Private Information.

176. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class members have suffered injuries and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

177. Plaintiffs incorporate by reference paragraphs 1 through 145 as if fully set forth herein.

178. Plaintiffs and Class Members were required to provide their PII/PHI to Defendant as a condition of receiving services from Defendant. Plaintiffs and Class Members provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's services.

179. Plaintiffs and Class Members reasonably understood that a portion of the funds they paid would be used to pay for adequate cybersecurity measures.

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

181. Plaintiffs and the Class Members accepted Defendant's offers by disclosing their PII/PHI to Defendant or its third-party agents in exchange for services.

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

183. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiffs and Class Members' PII/PHI.

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

185. After all, Plaintiffs and Class Members would not have entrusted their PII/PHI to Defendant in the absence of such an agreement with Defendant.

186. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

187. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain.

In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

189. Defendant materially breached the contracts it entered with Plaintiffs and Class Members by: failing to safeguard their information; failing to notify them promptly of the intrusion into its computer systems that compromised such information; failing to comply with industry standards; failing to comply with the legal obligations necessarily incorporated into the agreements; and failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

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

191. Defendant's material breaches were the direct and proximate cause of Plaintiffs and Class Members' injuries (as detailed *supra*).

192. And, on information and belief, Plaintiffs PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

193. Plaintiffs and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

194. Plaintiffs incorporate by reference paragraphs 1 through 145 as if fully set forth herein.

195. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

196. Defendant owed a duty to its current and former consumers, including Plaintiffs and the Class, to keep this information confidential.

197. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class Members' PII/PHI is highly offensive to a reasonable person.

198. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

199. The Data Breach constitutes an intentional interference with Plaintiffs and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

200. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

201. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

202. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

203. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

204. And, on information and belief, Plaintiffs PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

205. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

206. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiffs and the Class.

207. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class Members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

208. Plaintiffs incorporate by reference paragraphs 1 through 145 as if fully set forth herein.

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

210. Plaintiffs and Class Members conferred a benefit upon Defendant. After all, Defendant benefited from (1) using their PII/PHI to provide services, and (2) accepting payment.

211. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class Members.

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

213. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs and Class Members' PII/PHI.

214. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

215. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs and Class Members' (1) PII/PHI and (2) payment because Defendant failed to adequately protect their PII/PHI.

216. Plaintiffs and Class Members have no adequate remedy at law.

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

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

218. Plaintiffs incorporate by reference paragraphs 1 through 145 as if fully set forth herein.

219. Given the relationship between Defendant and Plaintiffs and Class Members, where Defendant became guardian of Plaintiffs and Class Members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs and Class Members' PII/PHI; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

220. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

221. Because of the highly sensitive nature of the PII/PHI, Plaintiffs and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

222. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs and Class Members' PII/PHI.

223. Defendant also breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

224. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SEVENTH CAUSE OF ACTION
Violation of the Maryland Consumer Protection Act
Md. Code Ann., Com. Law § 13-101, *et seq*.
(On Behalf of Plaintiffs and the Class)

225. Plaintiffs incorporate by reference paragraphs 1 through 145 as if fully set forth herein.

226. The Maryland Consumer Protection Act, Md. Code Ann., Com. Law § 13-101, *et seq*. ("MCPA"), applies to Defendant because Defendant is headquartered in Maryland and does substantial business in Maryland.

227. Plaintiffs and Class Members all constitute consumers under the MCPA.

228. The MCPA prohibits "any unfair, abusive, or deceptive trade practice[.]" Md. Code Ann., Com. Law § 13-303.

229. Defendant violated the MCPA by, *inter alia*: failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' PII/PHI, which was a direct and proximate cause of the Data Breach; 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; failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*., which was a direct and proximate cause of the Data Breach; omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Class Members' PII/PHI; and 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 Plaintiffs and Class Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

230. Moreover, Defendant violated the MCPA by failing to comply with the Maryland Personal Information Protection Act, Md. Comm. Code §§ 14-3501, *et seq*. ("PIPA"). Specifically, Defendant violated PIPA by, *inter alia*: failing to "protect personal information from unauthorized access, use, modification, or disclosure"; failing to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned, maintained, or licensed"; failing to require its third-party service providers (if any) to "require by contract that the third party implement and maintain reasonable security procedures and practices"; and failing to provide notice to Plaintiffs and Class Members "as reasonably practicable, but not later than 45 days after the business discovers or is notified of the breach of the security of a system[.]"

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

232. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its omissions.

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

234. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiffs and Class Members' rights.

235. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII/PHI.

236. And, on information and belief, Plaintiffs PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

237. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law.

PRAYER FOR RELIEF

Plaintiffs and Class Members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

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

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

D. Enjoining Defendant from further unfair and/or deceptive practices;

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

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

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

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

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

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Dated: June 11, 2025

By: */s/ Duane O. King*

Duane O. King, Bar # 19430
THE LAW OFFICES OF DUANE O. KING, P.C.
1001 L St. SE
Washington, DC 20003
Telephone: (202) 931-6252
dking@dkinglaw.com

Leigh S. Montgomery
Texas Bar No. 24052214
EKSM, LLP
4200 Montrose, Ste. 200
Houston, Texas 77006
Phone: (888) 350-3931
lmontgomery@eksm.com

Attorneys for Plaintiff Christensen

Duane O. King, Bar # 19430
THE LAW OFFICES OF DUANE O. KING, P.C.
803 W Broad Street Suite
210 Falls Church, VA 22046
Telephone: (202) 931-6252
dking@dkinglaw.com

Raina Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

Attorneys for Plaintiff Girgis

Thomas A. Pacheco (Bar No. 1712140091)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
900 W Morgan Street
Raleigh, NC 27603
T: (212) 946-9305
tpacheco@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20015
Phone: 866.252.0878
dlietz@milberg.com

Leanna A. Loginov*
SHAMIS & GENTILE, P.A.
14 NE 1st Ave, Suite 705
Miami, FL 33132
Tel: (305) 479-2299
Email: lloginov@shamisgentile.com

Attorneys for Plaintiff Sikaczowski

Thomas A. Pacheco (Bar No. 1712140091)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
900 W Morgan Street
Raleigh, NC 27603
T: (212) 946-9305
tpacheco@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20015
Phone: 866.252.0878
dlietz@milberg.com

Attorneys for Plaintiff Scott

**Pro Hac Vice* forthcoming

ClassAction.org