UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF GEORGIA
MACON DIVISION

PING WANG, EMILY LEHNES, EMILY RAMOS, JENNIFER KILKUS, and JOHN DOE, individually and on behalf of all others similarly situated, Plaintiff, v. THE CORPORATION OF MERCER UNIVERSITY, Defendant.	Case No. 5:23-cv-00193-TES **CONSOLIDATED CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Ping Wang, Ana Lehnes, Emily Lehnes, Emily Ramos, Jennifer Kilkus, and John Doe ("Plaintiffs") bring this class action against Defendant The Corporation of Mercer University ("Mercer University" or "Defendant") and allege the following based on personal knowledge and information and belief based on the investigation of counsel.

I. NATURE OF THE ACTION

1. Mercer University is a private research university that enrolls over 9,000 students in 12 colleges and schools. Mercer University's main campus is in Macon, Georgia. Mercer University's financial endowments surpassed half a billion dollars in 2021.[1]

2. Plaintiffs and the Class Members (as further defined below) have had their personally identifiable information exposed as a result of Mercer University's inadequately secured computer network. Personally identifiable information ("PII") refers to identifiers that

[1] https://den.mercer.edu/mercer-university-endowment-surpasses-half-billion-dollar-mark/ (last accessed October 3, 2023).

can be used to distinguish or trace an individual's identity. PII is particularly sensitive and, therefore, valuable in the wrong hands.

3. This class action seeks to redress Mercer University's unlawful, willful, and wanton failure to protect the PII of Plaintiffs and the Class Members. Indeed, due to Defendant's woefully inadequate security measures—including its failure to utilize basic encryption on sensitive data—the PII of approximately 93,512 individuals was exposed in an avoidable data breach of Defendant's network (the "Data Breach" or "Breach").[2]

4. The Data Breach was discovered by at least April 5, 2023, when Mercer University became aware of suspicious activity on its computer systems.[3] Based on a subsequent investigation, Mercer University confirmed that cybercriminals had infiltrated its inadequately secured network *months* earlier. Through this infiltration, cybercriminals gained undetected, and seemingly unfettered access, to scores of sensitive information. Indeed, Mercer University has admitted that unauthorized cybercriminals "accessed" files containing the confidential PII of Plaintiffs and Class Members between February 12, 2023 and February 24, 2023.[4] Mercer University also confirmed that such PII was "removed from its systems without authorization."[5]

5. According to Mercer University, the PII stolen in the Data Breach includes names, Social Security numbers, and driver's license numbers.[6]

---

[2] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/0b7ed19f-c57a-4d16-8091-3d97008af87d.shtml (last accessed October 3, 2023).
[3] *See* https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-308.pdf (last accessed October 3, 2023).
[4] *Id.*
[5] https://den.mercer.edu/mercer-university-statement-on-data-incident/ (last accessed October 3, 2023).
[6] *Id.*

6. Plaintiffs and Class Members—who are current and former students and employees of Mercer University—entrusted their PII to Mercer University with the mutual understanding that Defendant would take reasonable measures to protect it against unauthorized disclosure or access.

7. Due to Defendant's negligence, cybercriminals obtained sensitive information that could be used to commit identity theft and wreak havoc on the financial and personal lives of tens of thousands of individuals.

8. According to postings on the dark web, the Akira ransomware gang has taken credit for infiltrating Mercer University's computer network and has posted the PII stolen in the Data Breach on the dark web.[7] As part of its posting, the Akira gang stated that Mercer University had refused to pay the ransom.[8]

9. For the rest of their lives, Plaintiffs and the Class Members will have to deal with the danger of identity thieves possessing and misusing their PII. Plaintiffs and Class Members will have to spend time responding to the Breach and are at an immediate, imminent, and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their PII, loss of privacy, and/or additional damages as described below.

---

[7] *See* https://cybernews.com/news/mercer-university-data-breach/ (last accessed October 3, 2023); *see also* https://therecord.media/cyberattacks-chattanooga-state-mercer-university (last accessed October 3, 2023).

[8] *See* https://cybernews.com/news/mercer-university-data-breach/ (last accessed October 3, 2023).

10. Plaintiffs bring this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, disgorgement, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

Plaintiffs

11. Plaintiff Ping Wang is a citizen of Georgia. Plaintiff is a former student of Mercer University. On or around May 19, 2023, Plaintiff received a breach notification letter from Mercer University informing her that her PII, including name in combination with Social Security Number and/or driver's license number, had been accessed by cybercriminals during the Data Breach.

12. Plaintiff Emily Lehnes is a citizen of Georgia. Plaintiff is a former student of Mercer University. On or around May 19, 2023, Plaintiff received a breach notification letter from Mercer University informing her that her PII, including name in combination with Social Security Number and/or driver's license number, had been accessed by cybercriminals during the Data Breach.

13. Plaintiff Emily Ramos is a citizen of Georgia. Plaintiff is a former student of Mercer University. On or around May 19, 2023, Plaintiff received a breach notification letter from Mercer University informing her that her PII, including name in combination with Social Security Number and/or driver's license number, had been accessed by cybercriminals during the Data Breach.

14. Plaintiff Jennifer Kilkus is a citizen of Connecticut. Plaintiff is a former employee of Mercer University. On or around May 19, 2023, Plaintiff received a breach notification letter

from Mercer University informing her that her PII, including name in combination with Social Security Number and/or driver's license number, had been accessed by cybercriminals during the Data Breach.

15. Plaintiff John Doe is a citizen of Georgia. Plaintiff is a former student of Mercer University. On or around May 19, 2023, Plaintiff received a breach notification letter from Mercer University informing him that his PII, including name in combination with Social Security Number and/or driver's license number, had been accessed by cybercriminals during the Data Breach.

Defendant

16. Defendant The Corporation of Mercer University operates a private university, Mercer University, that enrolls more than 9,000 students in 12 colleges and schools, with its principal campus in Macon, Georgia.

III. JURISDICTION AND VENUE

17. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

18. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, it regularly transacts business in this District, and many Class Members reside in this District. Venue is likewise proper as to Defendant in this District because Defendant employs a significant number of Class Members in this District, and a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2).

IV. FACTUAL ALLEGATIONS

A. Background and the Data Breach

19. Mercer University is a private university that enrolls over 9,000 students in 12 colleges and schools. Mercer University's financial endowments surpassed half a billion dollars in 2021.[9]

20. Upon information and belief, in the course of collecting PII from its students and employees, including Plaintiffs, Defendant promised to ensure that confidentiality and adequate security would be provided for such data through its applicable privacy policy, assurances, and other disclosures in compliance with statutory privacy requirements.

21. Indeed, Defendant's Privacy Policy assures: "Your information will be held with the utmost care and will not be used for anything other than official business."[10] Additionally, Mercer University assures students and employees: "Mercer's IT department has implemented industry-standard network and system security measures to ensure our faculty, staff, and students are protected from computer security breaches and vulnerabilities."[11]

22. Plaintiffs and the Class Members, as students and employees of Defendant, relied on such promises and on this sophisticated entity to keep their sensitive PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information.

---

[9] https://den.mercer.edu/mercer-university-endowment-surpasses-half-billion-dollar-mark/ (last accessed October 3, 2023).

[10] *Privacy Policy*, https://www.mercer.edu/privacy-policy/#:~:text=Any%20and%20all%20information%20collected,anything%20other%20than%20official%20business (last accessed October 3, 2023)

[11] https://it.mercer.edu/student/security/security_alerts.htm (last accessed October 3, 2023).

23. In the course of their student or employment relationship with Defendant, Plaintiffs, and Class Members were required to provide, and did provide, Defendant with at least the following PII:

a. names;

b. dates of birth;

c. gender;

d. Social Security numbers;

e. addresses;

f. telephone numbers; and

g. email addresses.

24. Defendant had a duty to ensure that reasonable measures were taken to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

25. In the notice of Data Breach letters (all of which are virtually identical and will be referred to herein collectively as the "Notice Letter") sent to Plaintiffs and Class Members, Defendant informs Plaintiffs and Class Members that the Data Breach was discovered on April 5, 2023 when Mercer University "learned of [an] intrusion."[12] Mercer University's subsequent investigation confirmed that one or more unauthorized cybercriminals "accessed certain files stored on Mercer's computer servers" between February 12, 2023 and February 24, 2023.[13] The investigation further confirmed that these accessed files contained the PII of 93,512 individuals, including their names, Social Security numbers, and/or driver's license numbers.[14]

[12] *See* https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-308.pdf (last accessed October 3, 2023).
[13] *Id.*
[14] *Id.*

26. Omitted from the Notice Letter was any explanation of: (i) why it took Defendant *months* after the unauthorized access to even detect that its system had been infiltrated, (ii) whether further unauthorized access from these same cybercriminals was successfully prevented, (iii) the details of the root cause of the Data Breach, (iv) the vulnerabilities exploited that facilitated the Data Breach, and (v) the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

27. Indeed, it was only in a separate statement that Mercer University confirmed that the PII was, in fact, "***removed*** from its systems without authorization."[15]

28. Similarly, separate media sources revealed that the stolen PII had been ***posted and made available on the dark web***.[16]

29. Upon information and belief, the cyberattack was targeted at Defendant via its outside counsel, due to Defendant's status as a university that collects, creates, and maintains PII on various computer networks and/or systems.

30. Because of this targeted cyberattack, data thieves could gain access to and obtain data from Defendant that included the PII of Plaintiffs and Class Members.

31. As evidenced by the Data Breach's occurrence, Mercer University's network was not protected by sufficient multi-layer data security technologies or effective firewalls.

---

[15] https://den.mercer.edu/mercer-university-statement-on-data-incident/ (last accessed October 3, 2023).

[16] https://cybernews.com/news/mercer-university-data-breach/ (last accessed October 3, 2023); *see also* https://therecord.media/cyberattacks-chattanooga-state-mercer-university (last accessed October 3, 2023).

32. Similarly, based on the months-long delayed discovery of the intrusion, it is evident that Mercer University's network, including portions that stored Plaintiffs' and Class Members' PII, did not have effective endpoint detection.

33. Further, the fact that PII was accessed and obtained in the Data Breach demonstrates that the PII contained in the infiltrated network was not encrypted. Had the information been properly encrypted, the data thieves would have accessed only unintelligible data.

34. In addition, because the Data Breach was perpetrated through a successful ransomware attack,[17] it is evident that Mercer University had inadequate malware and ransomware protections in place.

35. As a result of Defendant's failure to implement reasonable industry-standard data security measures, Plaintiffs' PII was accessed and stolen in the Data Breach. Plaintiffs' and Class Members' PII was then posted and made available on the dark web because Mercer University refused to expend money to retrieve the PII.[18]

36. Due to the actual and imminent risk of identity theft as a result of the Data Breach, Plaintiffs, and Class Members must, as Defendant's Notice Letter provides a list of steps Plaintiffs and Class Members should take to mitigate the risks resulting from the Data Breach, including the advice to "be vigilant" and to review and monitor their "accounts statements and

[17] https://cybernews.com/news/mercer-university-data-breach/ (last accessed October 3, 2023).
[18] *See* https://cybernews.com/news/mercer-university-data-breach/ (last accessed October 3, 2023); *see also* https://therecord.media/cyberattacks-chattanooga-state-mercer-university (last accessed October 3, 2023).

credit reports for any unauthorized activity over the next 12-24 months."[19] The Notice Letter also encourages Plaintiffs and Class Members to freeze their credit temporarily.[20]

37. In the Notice Letter, Defendant makes an offer of one-year of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII.

38. That Defendant is encouraging Plaintiffs and Class Members to enroll in credit monitoring and identity theft protection services, and is warning Plaintiffs to be on guard for data misuse, is an acknowledgment that cybercriminals obtained the Plaintiffs' PII and thereby subjects Plaintiffs and Class Members to a substantial and imminent threat of fraud and identity theft.

39. Defendant had obligations created by contract, state and federal law, common law, and industry standards to keep Plaintiffs' and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

40. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiffs' and the other Class Members' PII from unauthorized disclosure.

41. Defendant also failed to provide timely notice to Plaintiffs and Class Members.

42. Defendant's actions represent a flagrant disregard of the Class Members' rights, both as to privacy and property.

---

[19] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-308.pdf (last accessed October 3, 2023).
[20] *Id.*

B. Plaintiffs' Experiences as a Result of the Breach

Plaintiff Ping Wang

43. Plaintiff Wang is a former student of Mercer University.

44. On or around May 19, 2023, Plaintiff Wang received a breach notification letter from Mercer University informing her that her PII, including name in combination with Social Security Number and/or driver's license number, had been identified as having been accessed by cybercriminals during the Data Breach.

45. Plaintiff Wang's PII was entrusted to Defendant for educational services with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

46. Because of the Data Breach, Plaintiff Wang's PII is now in the hands of cybercriminals. Plaintiff Wang and all Class Members are now imminently at risk of crippling future identity theft and fraud.

47. Plaintiff Wang and Class Members have already experienced data misuse because their PII has now been posted on the dark web.[21]

48. Since the Data Breach, Plaintiff Wang has also noticed an uptick in spam calls and has received mailings that reference PII she keeps confidential.

49. As a result of the Data Breach, Plaintiff Wang has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff Wang has spent time researching the facts and scope of the Data Breach, monitoring her accounts and personal information, placing a lock on her credit, reviewing her credit reports, closely monitoring suspicious calls and correspondence, and taking other steps in an attempt to mitigate the adverse consequences of the

[21] *See* https://cybernews.com/news/mercer-university-data-breach/ (last accessed October 3, 2023).

Data Breach. All of these actions have taken several hours aways from Plaintiff Wang's valuable time and that she otherwise would have spent on other activities, including but not limited to work and/or time with her family. The letter Plaintiff Wang received from Mercer University specifically encouraged her to take these actions.

50. Plaintiff Wang has been careful to protect and monitor her identity. Her PII has not been compromised in any other data breach to the best of her knowledge.

51. As a result of the Data Breach, Plaintiff Wang has experienced a noticeable increase in anxiety due to the loss of her privacy and anxiety over the impact of cybercriminals accessing, using, and selling her PII.

52. Plaintiff Wang anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

53. Plaintiff Wang has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

54. Plaintiff Wang has suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Wang's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Wang's PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff Wang's PII that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Wang should have received from Defendant and Defendant's defective

and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff Wang's PII; and (e) continued risk to Plaintiff Wang's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Emily Lehnes

55. Plaintiff Lehnes is a former student of Mercer University.

56. On or around May 19, 2023, Plaintiff Lehnes received a breach notification letter from Mercer University informing her that her PII, including name in combination with Social Security Number and/or driver's license number, had been identified as having been accessed by cybercriminals during the Data Breach.

57. Plaintiff Lehnes' PII was entrusted to Defendant for educational services with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

58. Because of the Data Breach, Plaintiff Lehnes' PII is now in the hands of cybercriminals. Plaintiff Lehnes and all Class Members are now imminently at risk of crippling future identity theft and fraud.

59. Plaintiff Lehnes and Class Members have already experienced data misuse because their PII has now been posted on the dark web.[22] Indeed, following the Data Breach, Plaintiff Lehnes was notified by Experian that her information had been found on the dark web.

60. As a result of the Data Breach, Plaintiff Lehnes has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff Lehnes has spent time researching

[22] *See* https://cybernews.com/news/mercer-university-data-breach/ (last accessed October 3, 2023).

the facts and scope of the Data Breach, researching and enrolling in credit monitoring identity theft protection, contacting credit bureaus to freeze her credit, monitoring her financial accounts for suspicious activity, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. All of these actions have taken several hours aways from Plaintiff Lehnes' valuable time and that she otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Lehnes' letter from Mercer University specifically encouraged her to take these actions.

61. Plaintiff Lehnes anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

62. Plaintiff Lehnes has been careful to protect and monitor her identity. Her PII has not been compromised in any other data breach to the best of her knowledge.

63. Plaintiff Lehnes, as a result of the Data Breach, has increased anxiety for their loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling her PII.

64. Plaintiff Lehnes has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

65. Plaintiff Lehnes has suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Lehnes' valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Lehnes' PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff Lehnes' PII that was entrusted to Defendant with the understanding that Defendant would

safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Lehnes should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff Lehnes' PII; and (e) continued risk to Plaintiff Lehnes' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Emily Ramos

66. Plaintiff Ramos is a former student of Mercer University.

67. On or around May 19, 2023, Plaintiff Ramos received a breach notification letter from Mercer University informing her that her PII, including name in combination with Social Security Number and/or driver's license number, had been identified as having been accessed by cybercriminals during the Data Breach.

68. Plaintiff Ramos's PII was entrusted to Defendant for educational services with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

69. Because of the Data Breach, Plaintiff Ramos's PII is now in the hands of cybercriminals. Plaintiff Ramos and all Class Members are now imminently at risk of crippling future identity theft and fraud.

70. Plaintiff Ramos and Class Members have already experienced data misuse by the fact that their PII has now been posted on the dark web.[23]

71. As a result of the Data Breach, Plaintiff Ramos has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff Ramos has spent time researching the facts and scope of the Data Breach, enhancing the robustness of the credit monitoring services she uses, monitoring her accounts and personal information, reviewing her credit monitoring reports, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach.

72. Indeed, Plaintiff Ramos has spent many hours each month since the Data Breach reviewing her accounts, and checking financial reports. She has considerable investments that a credit freeze would impact, and the hours spent are precautions to avoid having a credit freeze that may negatively impact those investments.

73. All of these actions have taken several hours aways from Plaintiff Ramos's valuable time and that she otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Ramos's letter from Mercer University specifically encouraged her to take these actions.

74. Plaintiff Ramos has been careful to protect and monitor her identity. Her PII has not been compromised in any other data breach to the best of her knowledge.

75. As a result of the Data Breach, Plaintiff Ramos has experienced a noticeable increase in anxiety due to the loss of her privacy and anxiety over the impact of cybercriminals accessing, using, and selling her PII.

---

[23] *See* https://cybernews.com/news/mercer-university-data-breach/ (last accessed October 3, 2023).

76. Plaintiff Ramos anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

77. Plaintiff Ramos has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

78. Plaintiff Ramos has suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Ramos's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Ramos's PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff Ramos's PII that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Ramos should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff Ramos's PII; and (e) continued risk to Plaintiff Ramos's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff Jennifer Kilkus

79. Plaintiff Kilkus is a former employee of Defendant's, who taught at a course at Mercer University in 2016 and 2018.

80. On or around May 19, 2023, Plaintiff Kilkus received a breach notification letter from Mercer University informing her that her PII, including name in combination with Social Security Number and/or driver's license number, had been identified as having been accessed by cybercriminals during the Data Breach.

81. Plaintiff Kilkus's PII was entrusted to Defendant for employment opportunities with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

82. Because of the Data Breach, Plaintiff Kilkus's PII is now in the hands of cybercriminals. Plaintiff Kilkus and all Class Members are now imminently at risk of crippling future identity theft and fraud.

83. Plaintiff Kilkus and Class Members have already experienced data misuse because their PII has now been posted on the dark web.[24]

84. As a result of the Data Breach, Plaintiff Kilkus has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff Kilkus has spent time researching the facts and scope of the Data Breach, closely monitoring her accounts and personal information, enrolling in credit monitoring services, reviewing her credit reports, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach.

85. Plaintiff Kilkus estimates that, to date, these actions have taken at least 5 hours of her valuable time that she otherwise would have spent on other activities, including but not limited to work and/or recreation. She now must continuously monitor her credit reports and bank accounts for fraud. Plaintiff Kilkus's letter from Mercer University specifically encouraged her to take these actions.

---

[24] *See* https://cybernews.com/news/mercer-university-data-breach/ (last accessed October 3, 2023).

86. Plaintiff Kilkus has been careful to protect and monitor her identity. Her PII has not been compromised in any other data breach to the best of her knowledge.

87. As a result of the Data Breach, Plaintiff Kilkus has experienced a noticeable increase in anxiety due to the loss of her privacy and anxiety over the impact of cybercriminals accessing, using, and selling her PII.

88. Plaintiff Kilkus anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

89. Plaintiff Kilkus has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

90. Plaintiff Kilkus has suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Kilkus's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Kilkus's PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff Kilkus's PII that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Kilkus should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff Kilkus's PII; and (e) continued risk to Plaintiff Kilkus's PII, which remains in the possession of Defendant and which is subject to further breaches so

long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

Plaintiff John Doe

91. Plaintiff Doe is a former student of Mercer University. He attended Mercer University between August 2020 and May 2023.

92. On or around May 19, 2023, Plaintiff Doe received a breach notification letter from Mercer University informing him that his PII, including name in combination with Social Security Number and/or driver's license number, had been identified as having been accessed by cybercriminals during the Data Breach.

93. Plaintiff Doe's PII was entrusted to Defendant for educational services with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

94. Because of the Data Breach, Plaintiff Doe's PII is now in the hands of cybercriminals. Plaintiff Doe and all Class Members are now imminently at risk of crippling future identity theft and fraud.

95. Plaintiff Doe and Class Members have already experienced data misuse because their PII has now been posted on the dark web.[25]

96. As a result of the Data Breach, Plaintiff Doe has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff Doe has spent time researching the facts and scope of the Data Breach, carefully monitoring his accounts and personal information, disputing fraudulent financial transactions, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach. All of these actions have taken several hours aways

[25] *See* https://cybernews.com/news/mercer-university-data-breach/ (last accessed October 3, 2023).

from Plaintiff Doe's valuable time and that he otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Doe's letter from Mercer University specifically encouraged him to take these actions.

97. Further, Plaintiff Doe has already experienced actual fraud and data misuse following the Data Breach. In May 2023, shortly after the Breach, Plaintiff Doe had three unauthorized credit card charges. Accordingly, Plaintiff Doe, upon information and belief, attributes these charges to the Data Breach.

98. Plaintiff Doe has been careful to protect and monitor his identity. To the best of his knowledge, his PII has not been compromised in any other data breach.

99. As a result of the Data Breach, Plaintiff Doe has experienced a noticeable increase in anxiety due to the loss of his privacy and anxiety over the impact of cybercriminals accessing, using, and selling his PII.

100. Plaintiff Doe anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

101. Plaintiff Doe has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

102. Plaintiff Doe has suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Doe's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff Doe's PII being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff Doe's PII that was entrusted to Defendant with the understanding that Defendant would safeguard this

information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Doe should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff Doe's PII; and (e) continued risk to Plaintiff Doe's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

C. Cyber Criminals Have Misused and Will Continue to Misuse Plaintiffs' PII

103. PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can and will be used in various ways for criminals to exploit Plaintiffs and the Class Members and profit off their misfortune.

104. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[26] For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[27] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and the Class Members.

---

[26] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last accessed October 3, 2023).

[27] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last accessed October 3, 2023).

105. Social Security numbers, which were compromised in the Data Breach, are particularly sensitive personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[28]
>
> [Emphasis added.]

106. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use It to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[29]

107. Moreover, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[28] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last accessed October 3, 2023).

[29] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION, www.ssa.gov/pubs/EN-05-10064.pdf (last accessed October 3, 2023).

108. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[30]

109. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, name, and date of birth.

110. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[31]

111. PII is such a valuable commodity to identity thieves that criminals will use it for years once it has been compromised.[32]

112. This was a financially motivated Breach, as the only reason the cyber criminals go through the trouble of running a targeted cyberattack against companies like Mercer University is to get information that they can monetize, including by holding the information as ransom

---

[30] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed October 3, 2023).

[31] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed October 3, 2023).

[32] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/gao-07-737.pdf (last accessed October 3, 2023).

and/or selling it on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[33] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[34]

113. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, they will use it if hackers gain access to PII.[35] Indeed, here, we know that the ***hackers have already posted the PII on the dark web***.

114. Hackers may not use the information immediately, but this does not mean it will not be used at all. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.[36]
>
> [Emphasis added.]

---

[33] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last accessed October 3, 2023).

[34] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last accessed October 3, 2023).

[35] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info (last accessed October 3, 2023).

[36] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO, July 5, 2007, https://www.gao.gov/assets/gao-07-737.pdf (last accessed October 3, 2023).

115. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[37]

116. The ramifications of Defendant's failure to keep its Class Members' PII secure are long-lasting and severe. Once that information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not appear for six to 12 months or even longer.

117. Further, criminals often trade stolen PII on the "cyber black-market" for years following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

118. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened. [38] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[39]

---

[37] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last accessed October 3, 2023).
[38] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last accessed October 3, 2023).
[39] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last accessed October 3, 2023).

119. Identity theft victims must spend countless hours and large amounts of money repairing the impact on their credit and protecting themselves in the future.[40]

120. Defendant's offer of limited identity monitoring to Plaintiffs and the Class is woefully inadequate and will not fully protect Plaintiffs from the damages and harm caused by its failures. There may be a time lag between when harm occurs versus when it is discovered and when PII is stolen and when it is used. Once the offered coverage has expired, Plaintiffs and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Mercer University's gross negligence. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity theft* (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[41] Nor can an identity monitoring service remove personal information from the dark web.[42] "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[43]

121. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of further harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the

---

[40] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf (last accessed October 3, 2023).
[41] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last accessed October 3, 2023).
[42] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last accessed October 3, 2023)
[43] *Id.*

Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more serious is the identity restoration that Plaintiffs and other Class Members must go through, which can include spending countless hours filing police reports, following Federal Trade Commission checklists, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps.

122. Plaintiffs and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

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

c. Improper disclosure of their PII;

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

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII and that identity thieves have already used that information to defraud other victims of the Data Breach;

f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

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

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

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

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

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

123. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[44] For example, PII can be sold at a price ranging from $40 to $200.[45] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[46]

124. Moreover, Plaintiffs and Class Members are interested in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by implementing industry-standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiffs' PII.

125. Plaintiffs and Class Members also have an interest in ensuring that their personal information that was provided to Mercer University is removed from Mercer University's unencrypted files.

126. Defendant acknowledged, in its letter to Plaintiffs and other Class Members, that the Data Breach would cause inconvenience to effected individuals by providing numerous steps for Class Members to take in an attempt to mitigate the harm caused by the Data Breach.[47]

---

[44] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited October 3, 2023).
[45] Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, Dec. 6, 2017, available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited October 3, 2023).
[46] *In the Dark*, VPN Overview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited October 3, 2023).
[47] *See* https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-308.pdf (October 3, 2023).

127. At Mercer University's suggestion, Plaintiffs are desperately trying to mitigate the damage that Mercer University has caused her. Given the kind of PII Mercer University made accessible to hackers, however, Plaintiffs are very likely to incur additional damages. This is exaggerated because cybercriminals have already posted the PII on the dark web.

128. Because identity thieves have her PII, Plaintiffs and all Class Members will need to have identity theft monitoring protection for several years and possibly for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[48]

129. None of this should have happened.

D. Defendant was Aware of the Risk of Cyber Attacks

130. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[49] Yahoo,[50] Marriott International,[51] Chipotle, Chili's, Arby's,[52] and others.[53]

---

[48] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html (October 3, 2023).

[49] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ (October 3, 2023).

[50] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html (October 3, 2023).

[51] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (October 3, 2023).

[52] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b (October 3, 2023).

131. Mercer University should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the PII that it collected and maintained.

132. Mercer University's assurance makes it evident that Mercer University recognized it had a duty to use reasonable measures to protect the PII that it collected and maintained. Yet, it appears that Mercer University did not meaningfully or comprehensively use reasonable measures, including those it claims to utilize.

133. Mercer University was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

E. Mercer University Could Have Prevented the Data Breach

134. Data breaches are preventable.[54] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[55] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[56]

135. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate

---

[53] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 08, 2022), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (October 3, 2023)

[54] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[55] *Id.* at 17.

[56] *Id.* at 28.

information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[57]

136. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[58] The guidelines establish that businesses should protect the confidential 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 for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

137. Upon information and belief, Mercer University failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Mercer University also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well-respected authorities in reasonable cybersecurity readiness.

---

[57] *Id.*

[58] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (October 3, 2023).

138. As the Federal Bureau of Investigation explains, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[59]

139. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

[59] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (October 3, 2023).

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[60]

140. Further, to prevent and detect cyberattacks, including the attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

[60] *Id.* at 3-4.

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[61]

141. In addition, to prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**

  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials

- **Thoroughly investigate and remediate alerts**

  - Prioritize and treat commodity malware infections as potential full compromise;

[61] *See* Protecting Against Ransomware (original release date Apr. 11, 2019), available at https://www.cisa.gov/news-events/news/protecting-against-ransomware (last accessed October 3, 2023).

- **Include IT Pros in security discussions**

    - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**

    - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**

    - Monitor for adversarial activities
        - Hunt for brute force attempts
        - Monitor for cleanup of Event Logs
        - Analyze logon events

- **Harden infrastructure**

    - Use Windows Defender Firewall
    - Enable tamper protection
    - Enable cloud-delivered protection
    - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[62]

142. Since Defendant was storing the Confidential Information of more than 80,000 individuals, Defendant could and should have implemented all of the above measures to prevent and detect malicious cyberattacks.

143. Specifically, among other failures, Mercer University had far too much confidential unencrypted information held on its systems. Such PII should have been segregated into an encrypted system.[63] Indeed, the United States Department of Health and Human

[62] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed October 3, 2023).
[63] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption (last accessed October 3, 2023).

Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information, stating, "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[64]

144. In sum, this Data Breach could have -been prevented through industry standard network segmentation and encryption of confidential information. Further, the Data Breach could have likely been prevented had Defendant utilized appropriate malware prevention and detection technologies.

F. Defendant Fails to Comply with FTC Guidelines

145. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

146. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, establishing cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

[64] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html (last accessed October 3, 2023).

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

148. The FTC has brought enforcement actions against employers for failing to protect employee data adequately and reasonably, 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.

149. These FTC enforcement actions include actions against employers over the compromised PII of their employees, like Defendant here.

150. Defendant failed to ensure that Plaintiffs' and Class Members' sensitive PII was stored in a network with basic data security practices.

151. Defendant's failure to ensure that reasonable and appropriate measures were in place to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

152. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. Defendant's Response to the Data Breach is Inadequate to Protect Plaintiffs and the Class

153. Defendant failed to inform Plaintiffs and Class Members of the Data Breach in time for them to protect themselves from identity theft.

154. The Data Breach took place in February 2023. Defendant stated that it discovered the Data Breach by at least April 5, 2023. And yet, Mercer University did not notify affected individuals until the end of May 2023. Even then, Mercer University failed to inform Plaintiffs and Class Members exactly what information was exposed in the Data Breach, leaving Plaintiffs and Class Members unsure as to the scope of information that was compromised.

155. During these intervals, the cybercriminals exploited the information while Mercer University was secretly investigating the Data Breach.

156. If Mercer University had investigated the Data Breach more diligently and reported it sooner, Plaintiffs and the Class could have taken steps to protect themselves sooner and to mitigate the damages caused by the Breach.

COMMON INJURIES AND DAMAGES

157. As a result of Defendant's negligence and the inadequate data security practices that existed on the breached IT network, the Data Breach, and the foreseeable consequences of PII ending up in possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; and (e) the continued risk to their PII, which remains in the possession and/or control of

Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

A. The Breach Increases Plaintiffs' and Class Member's Risk of Identity Theft

158. The unencrypted PII of Plaintiffs and Class Members is already for sale on the dark web, as is hackers' modus operandi. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

159. The link between a data breach and identity theft risk is simple and well-established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by, *inter alia*, posting and selling the stolen information on the black market to other criminals, who then utilize the information to commit a variety of identity theft related crimes discussed below.

160. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

161. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information

through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

162. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[65]

163. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

164. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still 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.

[65] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last accessed October 3, 2023).

165. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

166. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

167. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

B. Loss of Time to Mitigate the Risk of Identity Theft and Fraud

168. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the resource and asset of time has been lost.

169. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendant's Notice Letter encourages them, be "vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft and fraud.

170. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as signing up for credit monitoring and identity theft insurance, closing and opening new credit cards, and securing their financial accounts.

171. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in

which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[66]

172. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[67]

C. Diminution and Deprivation of Value of PII

173. PII is a valuable property right.[68] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts including heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

174. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[69]

175. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[70] In fact, the data marketplace is so

---

[66] *See* United States Government Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[67] *Id.*

[68] *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).

[69] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed October 3, 2023).

[70] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES (Nov. 5, 2019) https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed October 3, 2023).

sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[71] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[72]

176. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

177. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., Social Security numbers and names.

178. The fraudulent activity resulting from the Data Breach may not come to light for years.

179. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if the relevant data security systems were breached, including,

[71] *Home Page*, DATACOUP, https://datacoup.com/ (last accessed October 3, 2023).
[72] *Frequently Asked Questions*, NIELSEN COMPUTER & MOBILE PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed October 3, 2023).

specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

180. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

181. Defendant was, or should have been, fully aware of the unique type and the significant volume of data it allowed to be stored on a vulnerable network, amounting to potentially tens of thousands of individuals' detailed personal information and, thus, the significant number of individuals who the exposure of the unencrypted data would harm.

182. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to protect the PII of Plaintiffs and Class Members.

D. Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

183. Given the type of targeted attack in this case and sophisticated criminal activity, and the type of PII involved in this Data Breach, and given that the cybercriminals already have, and in all probability will continue, to place the stolen PII on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

184. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

185. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[73] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

186. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

187. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

E. Loss of Benefit of the Bargain

188. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When accepting educational services or employment opportunities from Defendant under certain terms, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying, or being paid less, for services and data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received educational services and employment positions that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

---

[73] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed October 3, 2023).

V. CLASS ACTION ALLEGATIONS

189. Plaintiffs incorporate by reference all preceding paragraphs as if fully restated here.

190. Plaintiffs bring this action against Mercer University on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of a nationwide class (the "Class") defined as follows:

> **Nationwide Class**
> All persons who Mercer University identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

191. Plaintiffs also seek to represent the following state subclass, defined as:

> **Georgia Subclass**
> All Georgia residents who Mercer University identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

192. The Nationwide Class and the state Subclass are referred to collectively as the Class. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

193. Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

194. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

195. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Defendant has reported that the total number of individuals affected in the Data Breach was 93,512 individuals.

196. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Mercer University's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Mercer University.

197. **Adequacy:** Plaintiffs are an adequate representative of the Class because Plaintiffs' interests do not conflict with the interests of the Class; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

198. **Superiority:** A class action is superior to 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 complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Mercer University's wrongdoing. Even if Class members 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 benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

199. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to safeguard Plaintiffs' and the Class's PII adequately;

c. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their PII, and whether it breached this duty;

d. Whether Mercer University breached its duties to Plaintiffs and the Class as a result of the Data Breach;

e. Whether Mercer University failed to provide adequate cyber security;

f. Whether Mercer University knew or should have known that its computer and network security systems were vulnerable to cyber attacks;

g. Whether Mercer University's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether Mercer University was negligent in permitting unencrypted PII of vast numbers of individuals to be stored within its network;

i. Whether Mercer University was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees, applicants, and business associates;

j. Whether Mercer University failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

k. Whether Mercer University continues to breach duties to Plaintiffs and the Class;

l. Whether Plaintiffs and the Class suffered injury as a proximate result of Mercer University's negligent actions or failures to act;

m. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief; and

n. Whether Mercer University's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

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

200. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

201. Defendant Mercer University solicited, gathered, and stored the PII of Plaintiffs and the Class.

202. Defendant had full knowledge of the sensitivity of the PII it maintained and of the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed. Defendant had a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiffs and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class Members had no ability to protect their PII that was in Mercer University's

possession. As such, a special relationship existed between Mercer University and Plaintiffs and the Class.

203. Defendant was well aware of the fact that cyber criminals routinely target corporations, particularly those servicing the health industry, through cyberattacks in an attempt to steal the collected PII.

204. Defendant owed Plaintiffs and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to safeguard such data reasonably and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

205. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

206. Defendant had duties to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to cyberattacks, including by encrypting documents containing PII, by not permitting documents containing unencrypted PII to be maintained on its systems, and other similarly common-sense precautions when dealing with sensitive PII. Additional duties that Mercer University owed Plaintiffs and the Class include:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;
b. To protect the PII in its possession using reasonable and adequate security procedures and systems;

c. To adequately and properly audit and test its systems;

d. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

e. To train its employees not to store PII for longer than absolutely necessary;

f. To implement processes to quickly detect a data breach, security incident, or intrusion; and

g. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

207. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect PII. Plaintiffs and Class Members are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards. Accordingly, Defendant has committed negligence *per se* by violating the FTC Act.

208. Various FTC publications and data security breach orders further form the basis of Defendant's duty.

209. Plaintiffs and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Mercer University. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiffs and the Class had entrusted to it.

210. Defendant breached its duties of care by failing to protect Plaintiffs' and Class Members' PII adequately. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit and test its computer systems to avoid cyberattacks;

d. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII, including maintaining it in an encrypted format;

e. Failing to consistently enforce security policies aimed at protecting Plaintiffs and the Class's PII;

f. Failing to implement processes to detect data breaches, security incidents, or intrusions quickly;

g. Failing to abide by reasonable retention and destruction policies for PII it collects and stores; and

h. Failing to promptly and accurately notify Plaintiffs and Class Members of the Data Breach that affected their PII.

211. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

212. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

213. The damages Plaintiffs and the Class have suffered (as alleged above) were and are reasonably foreseeable.

214. The damages Plaintiffs and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

215. Plaintiffs and the Class have suffered injury, including as described herein, and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of all Plaintiffs and the Class)

216. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

217. Through the use of Plaintiffs' and Class Members' PII, Defendant received monetary benefits, including payments and/or services.

218. Defendant collected, maintained, and stored the PII of Plaintiffs and Class Members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiffs and Class Members.

219. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

220. However, acceptance of the benefit under the facts and circumstances described herein makes it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits 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 decision to prioritize its own profits over the requisite data security.

221. Under the principle of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members because Defendant failed to implement the appropriate data management and security measures.

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

223. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to allow Defendant to have or maintain their PII.

224. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiffs and Class Members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably should have expended on data security measures to secure Plaintiffs' PII, (ii) time and expenses mitigating harms, (iii) diminished value of the PII, (iv) harms as a result of identity theft; and (v) an increased risk of future identity theft.

225. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiffs and the Class in direct violation of Plaintiffs' and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

226. Accordingly, Plaintiffs and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiffs and the Class.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of all Plaintiffs and the Class)

227. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

228. Defendant required Plaintiffs and Class Members to provide their PII in order for Mercer University to provide services or employment. In exchange, Defendant entered into implied contracts with Plaintiffs and Class Members in which Defendant implicitly agreed to comply with its statutory and common law duties to protect Plaintiffs' and Class Members' PII and to notify them in the event of a data breach timely.

229. Indeed, Defendant's Privacy Policy assures: "Your information will be held with the utmost care and will not be used for anything other than official business."[74] Additionally, Mercer University assures students and employees: "Mercer's IT department has implemented industry-standard network and system security measures to ensure our faculty, staff, and students are protected from computer security breaches and vulnerabilities."[75]

230. Plaintiffs and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

---

[74] *Privacy Policy*, https://www.mercer.edu/privacy-policy/#:~:text=Any%20and%20all%20information%20collected,anything%20other%20than%20official%20business (last accessed October 3, 2023)

[75] https://it.mercer.edu/student/security/security_alerts.htm (last accessed October 3, 2023).

231. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendant.

232. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

233. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members.

FOURTH CAUSE OF ACTION
VIOLATIONS OF THE GEORGIA SECURITY BREACH NOTIFICATION ACT,
GA. CODE ANN. § 10-1-912, *ET. SEQ.*
(On Behalf of Plaintiffs Wang, Lehnes, Ramos, and Doe and the Georgia Subclass)

234. Plaintiffs Wang, Lehnes, Ramos, and Doe ("Plaintiffs" for purposes of this count) bring this count on behalf of the Georgia Subclass.

235. Defendant is a business that owns or licenses computerized data that includes PII as defined by GA. CODE ANN. § 10-1-912(a).

236. Plaintiffs and Georgia Subclass Members' PII that was computerized in the Data Breach includes PII covered under GA. CODE ANN. § 10-1-912(a).

237. Defendant is required to accurately notify Plaintiffs and Georgia Subclass Members if it becomes aware of a breach of its data security systems that were reasonably likely to have caused unauthorized persons to acquire Plaintiffs' and Georgia Subclass Members' PII in the most expedient time possible and without unreasonable delay under GA. CODE ANN. § 10-1-912(a).

238. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated GA. CODE ANN. § 10-1-912(a).

239. As a direct and proximate result of Defendant's violations of GA. CODE ANN. § 10-1-912(a), Plaintiffs and Georgia Subclass Members suffered damages, as described above.

240. Plaintiffs and Georgia Subclass Members seek relief under GA. CODE ANN. § 10-1-912, including actual damages and injunctive relief.

FIFTH CAUSE OF ACTION
VIOLATIONS OF THE GEORGIA DECEPTIVE PRACTICES ACT,
GA. CODE ANN. § 10-1-912, *ET. SEQ.*
(On Behalf of Plaintiffs Wang, Lehnes, Ramos, and Doe and the Georgia Subclass)

241. Plaintiffs Wang, Lehnes, Ramos, and Doe ("Plaintiffs" for purposes of this count) and the Georgia Subclass incorporate by reference the foregoing paragraphs as if fully set forth herein.

242. Defendant, Plaintiff, and the Georgia Subclass members are "persons" within the meaning of the Georgia Deceptive Trade Practices Act ("Georgia DTPA"), Ga. Code Ann. § 10-1-370(5).

243. The Georgia DTPA states the following at Ga. Code Ann. § 10-1-372:

> (a) A person engages in a deceptive trade practice when, in the course of his business, vocation, or occupation, he: . . . (5) Represents that goods or services have . . . characteristics, . . . uses, [or] benefits . . . that they do not have; . . . (7) Represents that goods or services are of a particular standard, quality, or grade . . . if they are of another; . . . [or] (12) Engages in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.

244. Mercer University engaged in deceptive trade practices in violation of Ga. Code Ann. § 10-1- 372(a)(5), (7), and (12) by, among other things: (a) omitting and concealing the material fact that it did not employ reasonable measures to secure consumers' PII. Mercer University could and should have made a proper disclosure to consumers (including its clients and Georgia Subclass Members), during its enrollment process, or by any other means reasonably calcu-

lated to inform consumers of the inadequate data security; and (b) making implied or implicit representations that its data security practices were sufficient to protect consumers' PII.

245. Mercer University acquired consumers' PII during the enrollment process.

246. In doing so, Mercer University made implied or implicit representations that its data security practices were sufficient to protect consumers' PII.

247. Indeed, Defendant's Privacy Policy assures: "Your information will be held with the utmost care and will not be used for anything other than official business."[76] Additionally, Mercer University assures students and employees: "Mercer's IT department has implemented industry-standard network and system security measures to ensure our faculty, staff, and students are protected from computer security breaches and vulnerabilities."[77]

248. By virtue of accepting Plaintiffs' PII during the enrollment or employment process, Mercer University implicitly represented that its data security processes were sufficient to safeguard the PII.

249. The Georgia DTPA states that "[i]n order to prevail in an action under this part, a complainant need not prove . . . actual confusion or misunderstanding." Ga. Code Ann. § 10-1-372(b).

250. The Georgia DTPA further states: "A person likely to be damaged by a deceptive trade practice of another may be granted an injunction against it under the principles of equity and on terms that the court considers reasonable. Proof of monetary damage, loss of profits, or intent to deceive is not required." Ga. Code Ann. § 10-1-373(a).

---

[76] *Privacy Policy*, https://www.mercer.edu/privacy-policy/#:~:text=Any%20and%20all%20information%20collected,anything%20other%20than%20official%20business (last accessed October 3, 2023).

[77] https://it.mercer.edu/student/security/security_alerts.htm (last accessed October 3, 2023).

251. While Defendant provided notice of the Date Breach, Defendant has not provided sufficient details regarding the full scope of the Data Breach or any details related to the remedial measures it has taken to improve and more fully safeguard Plaintiffs' and Georgia Subclass Members' data from future compromise. As a result, Plaintiff, Georgia Subclass Members, and Mercer University's clients remain uninformed and confused as to the adequacy of Mercer University's data security and Mercer University's ability to protect the PII entrusted to it. Without adequate improvements, Plaintiffs' and Georgia Subclass Members' data remains at an unreasonable risk for future compromise.

252. Moreover, Defendant, through its omissions and Notice Letter, continues to represent and imply that its data security measures are adequate to protect the PII of Plaintiffs and the Georgia Subclass. Such continued representations and implications, without disclosure of the full scope of the Data Breach or remedial enhancements, place Plaintiffs and Georgia Subclass Members at future risk of harm, as Plaintiff, Georgia Subclass Members, and Mercer University's clients are not fully informed as to whether Mercer University's data security measures have been improved since the Data Breach. Mercer University's data systems have not been adequately improved by all available measures, and Plaintiffs and Georgia Subclass Members remain at an unreasonable risk from future cyberattacks.

253. Plaintiffs and the Georgia Subclass, therefore, are entitled to the injunctive relief sought herein because, among other things, Mercer University continues to retain their PII, future cyber-attacks targeting the same data are foreseeable, and Defendants have not provided sufficient notice identifying any remedial measures that will protect the data from future attack. Moreover, absent injunctive relief, Defendant will continue to misrepresent and imply that its

data systems adequately protect the PII of Plaintiffs and the Georgia Subclass from future cyberattacks without providing any firm details or basis to support these representations.

254. The Georgia DTPA states that the "court, in its discretion, may award attorney's fees to the prevailing party if . . . [t]he party charged with a deceptive trade practice has willfully engaged in the trade practice knowing it to be deceptive." Ga. Code Ann. § 10-1-373(b)(2). Mercer University willfully engaged in deceptive trade practices knowing them to be deceptive. Mercer University knew or should have known that its data security practices were deficient. This is true because, among other things, Mercer University was aware that entities responsible for collecting and maintaining large amounts of PII, including Social Security numbers and financial information, are frequent targets of sophisticated cyberattacks. Mercer University knew or should have known that its data security practices were insufficient to guard against those attacks.

255. The Georgia DTPA states that "[c]osts shall be allowed to the prevailing party unless the court otherwise directs." Ga. Code Ann. § 10-1-373(b). Plaintiffs and the Georgia Subclass are entitled to recover their costs of pursuing this litigation.

256. As a result of Mercer University's deceptive acts and practices, Plaintiffs and the Georgia Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and non-monetary damages, as alleged herein.

257. As a further result of Mercer University's deceptive acts and practices, Plaintiffs and the Georgia Subclass are at future risk of injury as a result of Mercer University's misrepresentations as to its data security practices and the lack of information Mercer University has provided regarding any enhancements to its data security.

258. Plaintiffs and the Georgia Subclass seek all monetary and non-monetary relief allowed by the Georgia DTPA, including injunctive relief and attorneys' fees.

SIXTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of all Plaintiffs and the Class)

259. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

260. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

261. Defendant owes duties of care to Plaintiffs and Class Members that require Defendant to secure their PII adequately.

262. Defendant still possesses Plaintiffs' and Class Members' PII.

263. Defendant does not specify in the Notice of Data Breach letters what steps they have taken to prevent a data breach from occurring again.

264. Plaintiffs and Class Members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

265. Plaintiff, therefore, seeks a declaration that (1) Defendant's existing security measures do not comply with its duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

i. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. Auditing, testing, and training their security personnel regarding any new or modified procedures;

iv. Segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. Conducting regular database scanning and security checks;

vi. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

vii. Purchasing credit monitoring services for Plaintiffs and Class Members for a period of ten years; and

viii. Meaningfully educating Plaintiffs and Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Complaint.

Dated: October 3, 2023

Respectfully submitted,

/s/ William B. Federman

William B. Federman*
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
wbf@federmanlaw.com

LAUKAITIS LAW LLC
Kevin Laukaitis*
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Interim Co-Lead Class Counsel

Brian P. Adams
Georgia Bar No. 142474
Mary Beth Hand
Georgia Bar No. 322826
ADAMS LAW FIRM
598 D.T. Walton Sr. Way
Macon, GA 31201
T: (478) 238-0231
brian@brianadamslaw.com
mbhand@brianadamslaw.com

Liaison Counsel for Plaintiffs and the Class

MURPHY LAW FIRM
A. Brooke Murphy*
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
T: (405) 389-4989
abm@murphylegalfirm.com

REESE LLP
Michael R. Reese
100 West 93rd Street, 16th Floor
New York, NY 10025
T: (212) 643-0500
F: (212) 253-4272

TURKE & STRAUSS LLP
Samuel J. Strauss
Raina Borrelli*
613 Williamson St., #201
Madison, WI 53703
T: (608) 237-1775
sam@turkestrauss.com
raina@turkestrauss.com

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
David K. Leitz
5335 Wisconsin Avenue NW
Washington, D.C. 20015-2052
T: (866) 252-0878
F: (202) 686-2877
dlietz@milberg.com

KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
Kenneth J. Grunfeld*
65 Overhill Road
Bala Cynwyd, PA 19044
T: (954) 525-4100
grunfeld@kolawyers.com

Additional Attorneys for Plaintiffs and the Class

**Admitted pro hac vice*

CERTIFICATE OF SERVICE

I hereby certify that on October 3, 2023, a copy of the foregoing was filed electronically. Service of this filing will be made on all ECF-registered counsel by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/ William B. Federman
William B. Federman