

2. Mercer has failed to comply with industry standards to protect information in its systems that contain PII, and has failed to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII had been compromised. Plaintiff seeks, among other things, orders requiring Mercer to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices and safeguards to prevent incidents like this in the future.

3. Mercer experienced a data security incident between February 12, 2023 and February 24, 2023 that involved Plaintiff's and other consumers' PII (the "Data Breach"). As a result, an unauthorized party accessed certain files and folders within the Defendant's systems and may have viewed, acquired, and/or exfiltrated data containing affected parties' PII. The security incident was wide-reaching, affecting a number of the Defendant's computer systems and compromising the PII of more than 93,000 people.

4. As a result of Defendant's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of criminals. Plaintiff and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiff and Class Members have

had to spend, and will continue to spend, significant time and money in the future to protect themselves due to the Defendant's failures.

5. Accordingly, Plaintiff, individually and on behalf of all others similarly situated, alleges claims for negligence and negligence *per se*, breach of implied contract, unjust enrichment, and injunctive/declaratory relief.

PARTIES

6. Plaintiff Emily Ramos is domiciled in Macon, Georgia and is a citizen of the State of Georgia. Plaintiff was formerly a law student at Mercer University. Plaintiff's PII was collected and maintained by Mercer and disclosed without authorization to an unknown and unauthorized third party as a result of the Data Breach. *See* Exhibit 1 attached hereto for a copy of the Notice Letter that Plaintiff received regarding the Data Breach.

7. Defendant Mercer University is a private university with its main campus in Macon, Georgia. Founded in 1833, and with an endowment of more than half a billion dollars, it is the oldest private university in the state and enrolls more than 9,000 students in 12 colleges and schools.¹ Due to the nature of the services it provides, Mercer regularly acquires and electronically stores PII

¹ *See* <https://den.mercer.edu/mercer-university-endowment-surpasses-half-billion-dollar-mark/> (last visited June 2, 2023).

belonging to students, prospective students, employees, and other consumers as part of the regular course of its business.

JURISDICTION AND VENUE

8. Jurisdiction is proper in this Court under 28 U.S.C. §1332(d), the Class Action Fairness Act. Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one class member is a citizen of a state different from Defendant.

9. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. §1367.

10. Defendant is headquartered and routinely conducts business in the State where this district is located, has sufficient minimum contacts in this State, and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

11. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims occurred within this District and Defendant does business in this Judicial District.

BACKGROUND AND FACTS

12. In May of 2023, Defendant publicly disclosed that it had “recently detected an incident involving unauthorized access to its computer network.”²

13. Defendant initiated an investigation and engaged cybersecurity experts to determine the size and scope of the breach. In April 2023, Mercer learned that between February 12, 2023 and February 24, 2023, there was a data security incident involving Plaintiff’s and class members’ PII.

14. Defendant and its cybersecurity experts then conducted an investigation that was completed in or about April 2023. The investigation determined that in fact, students’, employees’ and other consumers’ PII, including the Plaintiff’s PII, was put at risk, including names and Social Security numbers. The security incident was wide-reaching, affecting a number of the organization’s computer systems and compromising the PII of more than 93,0000 people.

15. Defendant mailed notification letters to all affected individuals informing them about the Data Breach. In these letters, Defendants offered affected individuals the opportunity to enroll in free credit monitoring and identity restoration services through a product sold by Experian.

² See <https://den.mercer.edu/mercer-university-statement-on-data-incident/> (last visited June 2, 2023).

16. The Notification Letters were deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, when Defendant first discovered the Data Breach, why sensitive information was stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the stolen data was encrypted or otherwise protected, and whether Defendant knows if the data has not been further disseminated.

17. Upon information and belief, the Akira ransomware gang posted on the dark web that Mercer was one of its victims, but Mercer's Notification Letters did not disclose any details regarding the Akira ransomware gang, or any other bad actor.

18. In deliberate disregard of the fact that the stolen sensitive information was accessed by an unauthorized third party, Mercer downplayed the seriousness of the incident by failing to take steps necessary to inform Plaintiff and Class Members that their data was in fact stolen by third party bad actors, and that Mercer, seemingly more out of an abundance of caution, wanted to make Plaintiff and Class Members aware of the Data Breach.

19. Mercer acknowledges that it is responsible to safeguard Plaintiff and Class Members' PII. It pledges that it takes privacy very seriously and makes numerous promises that it will maintain the security and privacy of PII.

20. The students and former students of Mercer entrusted their PII to Mercer with the mutual understanding that this highly sensitive private information was confidential and would be properly safeguarded from misuse and theft.

21. In addition, as an employer that provides educational services to students and benefits to employees, Mercer collects and stores highly sensitive medical and private health information (“PHI”) about individuals on its computer systems.

22. The privacy policy posted on Mercer’s website states: “Your information will be held with the utmost care and will not be used for anything other than official business.”³

23. By obtaining, collecting, using, and deriving a benefit from Plaintiff’s and Class Members’ PII, Mercer assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class Members’ PII from disclosure.

24. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and they rely on Mercer to keep this information

³ See <https://www.mercer.edu/privacy-policy/> (last visited June 2, 2023).

confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

25. Mercer was well aware that the PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes. As the Federal Trade Commission (FTC) recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and fraud.⁴ Indeed, a robust “cyber black market” exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

26. The ramifications of Defendant’s failure to keep PII secure are long lasting and severe. Once stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

27. 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.

⁴ Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited June 2, 2023).

28. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.⁵ This time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used, compounds an identity theft victim's ability to detect and address the harm.

29. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her 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.

30. Further, 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

⁵ *Identity Theft and Your Social Security Number*, Social Security Administrative, available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed June 2, 2023).

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.

31. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “The 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.”⁶

32. Defendant knew, or should have known, the importance of safeguarding PII entrusted to it and of the foreseeable consequences if its systems were breached. This includes the significant costs that would be imposed on individuals as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

33. Plaintiff and Class Members now face years of constant surveillance of their records. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

⁶ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited June 2, 2023).

34. Despite all of the publicly available knowledge of the continued compromises of PII, Mercer's approach to maintaining the privacy of the PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

35. In all contexts, time has constantly been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiff and Class Members should be spared having to deal with the consequences of Defendant's misfeasance.

36. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

37. The delay in identifying and reporting the Data Breach caused additional harm to Plaintiff and Class Members. Plaintiff was not timely notified of the Data Breach, depriving her and the Class of the ability to promptly mitigate potential adverse resulting consequences.

38. As a result of Mercer's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

- a. Actual identity theft;

- b. Unauthorized use and misuse of their PII;
- c. The loss of the opportunity to control how their PII is used;
- d. The diminution in value of their PII;
- e. The compromise, publication, and/or theft of their PII;
- f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- g. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- h. Costs associated with placing freezes on credit reports;
- i. Delay in receipt of tax refund monies or lost opportunity and benefits of electronically filing of income tax returns;
- j. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- k. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as it fails to undertake appropriate measures to protect the PII in its possession; and
- l. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

39. To date, Mercer has not yet disclosed full details of the Data Breach.

Without such disclosure, questions remain as to the full extent of the Data Breach,

the actual data accessed and compromised, and what measures, if any, it has taken to secure the PII still in its possession. Through this litigation, Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses any harms, and ensure Mercer has proper measures in place to prevent another breach from occurring in the future.

40. Mercer was expressly prohibited by the Federal Trade Commission Act (“FTC Act”) (15 U.S.C. §45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

41. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.⁷

⁷ Federal Trade Commission, *Start With Security: A Guide for Business*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed June 2, 2023).

42. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.⁸ The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

43. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

44. Mercer failed to properly implement basic data security practices. Its failure to employ reasonable and appropriate measures to protect against

⁸ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed June 2, 2023).

unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

45. Mercer was at all times fully aware of its obligation to protect PII and was also aware of the significant repercussions that would result from its failure to do so.

CLASS ACTION ALLEGATIONS

46. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of herself and all others similarly situated (the “Class”). Plaintiff proposes the following Class definition, subject to amendment as appropriate:

All individuals whose PII was maintained by Mercer and who were sent a notice of the 2023 Data Breach.

Plaintiff Emily Ramos also brings her claims on behalf of a Subclass of Georgia victims with subclass to be defined as follows:

All Georgia individuals whose PII was maintained by Mercer and who were sent a notice of the 2023 Data Breach.

47. Excluded from the Class are Defendant, Defendant’s subsidiaries and affiliates, its officers, directors, and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representatives, heirs,

successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

48. Plaintiff reserves the right to modify or amend the definition of the proposed Class and Subclass and/or to add classes or subclasses, if necessary, before this Court determines whether certification is appropriate.

49. Numerosity: The Class Members are so numerous that joinder of all Members is impractical. The Class is comprised of over 93,000 individuals. Defendant has the administrative capability through its computer systems and other records to identify all members of the Class and Subclass, and such specific information is not otherwise available to Plaintiff.

50. Commonality: The questions here are ones of common or general interest such that there is a well-defined community of interest among the Members of the Class and Subclass. These questions predominate over questions that may affect only individual class members because Mercer has acted on grounds generally applicable to the Class and Subclass. Such common legal or factual questions include, but are not limited to:

- a. Whether and to what extent Defendant had a duty to protect the PII of Class Members;
- b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII;

- c. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;
- d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;
- e. Whether Defendant failed to adequately safeguard the PII of Class Members;
- f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class Members' PII;
- g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- h. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- i. Whether Plaintiff and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;
- m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;
- n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach; and
- o. Whether Plaintiff and Class Members are entitled to additional identity theft protection.

51. Typicality: Plaintiff's claims are typical of the claims of the other members of the Class because Plaintiffs' PII, like that of every other Class Member, was not properly maintained or secured by Defendant. Plaintiff's claims

are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of Mercer. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

52. It is impracticable to bring the individual claims of the members of the Class and Subclass before the Court. Class treatment permits a large number of similarly situated persons or entities to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that numerous individual actions would engender. The benefits of the class mechanism, including providing injured persons or entities with a method for obtaining redress on claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action.

53. Adequacy of Representation: Plaintiff is a more than adequate representative of the Class in that Plaintiff's PII was compromised and has suffered damages. In addition:

- a. Plaintiff is committed to the vigorous prosecution of this action on behalf of herself and all others similarly situated and has retained competent counsel experienced in the prosecution of class actions and, in particular, class actions regarding data breaches;
- b. There is no conflict of interest between Plaintiff and the unnamed members of the Class or Subclass;
- c. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and
- d. Plaintiff's legal counsel have the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

54. Plaintiff knows of no difficulty to be encountered in the maintenance of this action that would preclude its maintenance as a class action.

55. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

56. Mercer has acted or refused to act on grounds generally applicable to the Class and Subclass, thereby making appropriate corresponding declaratory relief with respect to the Class and Subclass as a whole. Mercer's actions and

inactions challenged herein apply to and affect Class Members uniformly and hinges on its conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

57. Superiority of Class Action. The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against a large organization like Defendant. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

58. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage

since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

59. The litigation of the claims brought herein is manageable. Mercer's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

60. Adequate notice can be given to Class Members directly using information maintained in Mercer's records.

61. Unless a Class-wide injunction is issued, Mercer may continue in its failure to properly secure the PII of Class Members, may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and may continue to act unlawfully as set forth in this Complaint.

62. All conditions precedent to bringing this action have been satisfied and/or waived.

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

63. Plaintiff and the Class re-allege and incorporate by reference each and every preceding paragraph of this Complaint.

64. Defendant had a duty to exercise reasonable care to protect and secure Plaintiff's and the Class Members' PII.

65. Through its acts and omissions, Defendant violated its duty to use reasonable care to protect and secure Plaintiff's and Class Members' PII as set forth herein and as follows:

- a. Defendant failed to physically or electronically protect and secure Plaintiff's and Class Members' PII;
- b. Defendant retained Plaintiff's and Class Members' PII longer than was reasonably necessary; and,
- c. Defendant failed to disclose the security breach in the most expedient time possible and without unreasonable delay to Plaintiff and Class Members.

66. Defendant breached the duties owed to Plaintiff and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of information that resulted in the unauthorized access and

compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow its own privacy policies and practices.

67. It was reasonably foreseeable that Defendant's failure to exercise reasonable care to protect and secure Plaintiff's and Class Members' PII would result in an unauthorized third-party gaining access to, possession of, and control over such information for an unlawful purpose.

68. Defendant's failure to adequately protect Plaintiff's and Class Members' PII was negligent.

69. Plaintiff's and Class Members' PII constitute personal property and due to Defendant's negligence their PII was exposed or stolen, resulting in harm to Plaintiff and Class Members.

70. Defendant's negligence directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII and

Plaintiff and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described herein.

71. Section 5 of the FTCA prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Mercer or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Mercer’s duty.

72. Mercer violated Section 5 of the FTCA by failing to use reasonable measures to protect PII and not complying with the industry standards. Mercer’s conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a Data Breach.

73. Plaintiff and Members of the Class are consumers within the class of persons Section 5 of the FTCA was intended to protect.

74. Mercer’s violation of Section 5 of the FTCA constitutes negligence *per se*.

75. The harm that has occurred as a result of its conduct is the type of harm that the FTC Act was intended to guard against.

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

76. Plaintiff and the class re-allege and incorporate by reference each and every preceding paragraph of this Complaint.

77. When Plaintiff and members of the Class provided their personal information to Mercer, Plaintiff and members of the Class entered into implied contracts with Mercer pursuant to which Mercer agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their data had been breached and compromised.

78. Defendant required Plaintiff and class members to provide and entrust their PII and financial information as a condition of obtaining Defendant's services.

79. Plaintiff and Class members would not have provided and entrusted their PII and financial information to Mercer in the absence of the implied contract between them and Mercer.

80. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Mercer.

81. Mercer breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the personal information of Plaintiff

and members of the Class and by failing to provide timely and accurate notice to them that their personal information was compromised in and as a result of the Data Breach.

82. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of Mercer's breaches of the implied contracts between Mercer and Plaintiff and members of the Class.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

83. Plaintiff and the Class restate and reallege all proceeding allegations above as if fully set forth herein.

84. This count is brought in the alternative to Plaintiff's breach of contract count. If claims for breach of contract are ultimately successful, this count will be dismissed.

85. Plaintiff and Class members conferred a benefit on Mercer by way of customers' paying Mercer to maintain Plaintiff and Class members' personal information.

86. The monies paid to Mercer were supposed to be used by Mercer, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class members.

87. Mercer failed to provide reasonable security, safeguards, and protections to the personal information of Plaintiff and Class members, and as a result Mercer was overpaid.

88. Under principles of equity and good conscience, Mercer should not be permitted to retain the money because Mercer failed to provide adequate safeguards and security measures to protect Plaintiff's and Class members' personal information that they paid for but did not receive.

89. Mercer wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class members.

90. Mercer's enrichment at the expense of Plaintiff and Class members is and was unjust.

91. As a result of Mercer's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Mercer, plus attorneys' fees, costs, and interest thereon.

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

92. Plaintiff and the Class restate and reallege all proceeding allegations above as if fully set forth herein.

93. This cause of action is brought under 28 U.S.C. § 2201. This Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious as described in this Complaint.

94. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate, contrary to its assertion that it has confirmed the security of its network and its systems.

95. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of PII and remains at imminent risk that further compromises will occur in the future.

96. This Court should enter a judgment declaring, among other things, the following:

- a. Defendant owes a legal duty to secure PII and to timely notify those affected of the Data Breach; and
- b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure PII.

97. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect PII.

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

99. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Mercer if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Mercer of complying with an injunction by employing reasonable prospective data security measures and communicating those measures to the Class is relatively minimal, and it has a pre-existing legal obligation to employ such measures.

100. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Mercer, thus eliminating the additional injuries that would result to Plaintiff and to those whose PII would be further compromised.

101. Plaintiff and the Class, therefore, seek a declaration (1) that Mercer's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their obligations and duties of care, Mercer must implement and maintain reasonable security measures, including, but not limited to, the following:

- a. Ordering that Defendant engage 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;
- b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;
- d. Ordering that Defendant segment PII data by, among other things, creating firewalls and access controls so that if one area of Defendant's system is compromised, hackers cannot gain access to other portions of Defendant's systems;
- e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner all data not necessary for its provisions of services;
- f. Ordering that Defendant conduct regular computer system scanning and security checks;
- g. Ordering that Defendant routinely and continually conduct 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; and

- h. Ordering Defendant to meaningfully educate employees and 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.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all other similarly situated, prays for relief as follows:

- A. For an order certifying the Class and Subclass and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;
- B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- C. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;
- D. For an order of restitution and all other forms of equitable monetary relief;
- E. Declaratory and injunctive relief as described herein;
- F. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;
- G. Awarding pre- and post-judgment interest on any amounts awarded; and
- H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Date: June 5, 2023

Respectfully submitted,

BY: WEBB, KLASE & LEMOND, LLC

/s/ G. Franklin Lemond, Jr.

E. Adam Webb

Georgia Bar No. 743910

G. Franklin Lemond, Jr.

Georgia Bar No. 141315

1900 The Exchange, S.E.

Suite 480

Atlanta, Georgia 30339

(770) 444-9325

(770) 217-9950 (fax)

Adam@WebbLLC.com

Franklin@WebbLLC.com

Kenneth J. Grunfeld*

Kevin W. Fay*

GOLOMB SPIRT GRUNFELD

1835 Market Street, Suite 2900

Philadelphia, PA 19103

Phone: 215-985-9177

kgrunfeld@golomblegal.com

kfay@golomblegal.com

*Attorneys for Plaintiff and Proposed
Class*

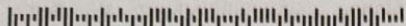
**Pro hac vice or applications for
admission to be filed*

Exhibit 1



May 19, 2023

1 AV *A-01-QQT-AM-19785-79



EMILY ANN RAMOS
1283 JEFFERSON TER
MACON GA 31201-6703



Dear Emily Ann Ramos:

Mercer University takes the security of our computer systems very seriously. Even so, like many thousands of organizations including hundreds of higher education institutions, we have now experienced an unlawful access into our system. This notice explains the incident, measures we have taken, and some additional steps you may consider taking in response.

Upon identifying the incident, we immediately secured the systems involved, alerted law enforcement, and launched an investigation. Through the investigation that began when we learned of the intrusion, we determined an unauthorized actor accessed certain files stored on Mercer's computer servers. These files included at least one record that contained your name, in combination with your Social Security number and/or driver's license number.

We are offering complimentary identity theft protection services through a one-year membership with Experian® IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks is completely free to you and enrolling in this program will not hurt your credit score. **For more information on Experian IdentityWorks Credit 3B, including instructions on how to activate your complimentary membership as well as some additional steps you can take to help protect yourself, please see the pages that follow this letter.** If you have any questions, please call 866-347-6455 between the hours of 8:00 a.m. and 5:30 p.m., Central Time, excluding major U.S. holidays.

Working with leading experts to help minimize the risk of events such as this from occurring in the future, we have taken, and will continue to take, steps to further enhance the security of our computer systems and the data we maintain.

Sincerely,

William D. Underwood
President

ELN-17792

CIVIL COVER SHEET

The JS44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

Emily Ramos, an individual, on behalf of herself and all others similarly situated,

DEFENDANT(S)

Mercer University

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF Bibb County
(EXCEPT IN U.S. PLAINTIFF CASES)

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT Bibb County
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

G. Franklin Lemond, Jr.
Webb, Klase & Lemond, LLC
1900 The Exchange SE, Suite 480
Atlanta, GA 30339
770-444-9594 - franklin@webbllc.com

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION
(PLACE AN "X" IN ONE BOX ONLY)

- 1 U.S. GOVERNMENT PLAINTIFF
- 2 U.S. GOVERNMENT DEFENDANT
- 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
- 4 DIVERSITY (INDICATE CITIZENSHIP OF PARTIES IN ITEM III)

III. CITIZENSHIP OF PRINCIPAL PARTIES
(PLACE AN "X" IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)
(FOR DIVERSITY CASES ONLY)

- | | | | | | |
|---------------------------------------|----------------------------|---|----------------------------|---------------------------------------|---|
| PLF | DEF | | PLF | DEF | |
| <input checked="" type="checkbox"/> 1 | <input type="checkbox"/> 1 | CITIZEN OF THIS STATE | <input type="checkbox"/> 4 | <input checked="" type="checkbox"/> 4 | INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE |
| <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | CITIZEN OF ANOTHER STATE | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 | INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE |
| <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | CITIZEN OR SUBJECT OF A FOREIGN COUNTRY | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 | FOREIGN NATION |

IV. ORIGIN (PLACE AN "X" IN ONE BOX ONLY)

- 1 ORIGINAL PROCEEDING
- 2 REMOVED FROM STATE COURT
- 3 REMANDED FROM APPELLATE COURT
- 4 REINSTATED OR REOPENED
- 5 TRANSFERRED FROM ANOTHER DISTRICT (Specify District)
- 6 MULTIDISTRICT LITIGATION - TRANSFER
- 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

28 U.S.C. §1332(d)

(IF COMPLEX, CHECK REASON BELOW)

- 1. Unusually large number of parties.
- 2. Unusually large number of claims or defenses.
- 3. Factual issues are exceptionally complex.
- 4. Greater than normal volume of evidence.
- 5. Extended discovery period is needed.
- 6. Problems locating or preserving evidence.
- 7. Pending parallel investigations or actions by government.
- 8. Multiple use of experts.
- 9. Need for discovery outside United States boundaries.
- 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT \$ _____ APPLYING IFP _____ MAG. JUDGE (IFP) _____
 JUDGE _____ MAG. JUDGE _____ (Referral) NATURE OF SUIT _____ CAUSE OF ACTION _____

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK

- 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK

- 110 INSURANCE
- 120 MARINE
- 130 MILLER ACT
- 140 NEGOTIABLE INSTRUMENT
- 151 MEDICARE ACT
- 160 STOCKHOLDERS' SUITS
- 190 OTHER CONTRACT
- 195 CONTRACT PRODUCT LIABILITY
- 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK

- 210 LAND CONDEMNATION
- 220 FORECLOSURE
- 230 RENT LEASE & EJECTMENT
- 240 TORTS TO LAND
- 245 TORT PRODUCT LIABILITY
- 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK

- 310 AIRPLANE
- 315 AIRPLANE PRODUCT LIABILITY
- 320 ASSAULT, LIBEL & SLANDER
- 330 FEDERAL EMPLOYERS' LIABILITY
- 340 MARINE
- 345 MARINE PRODUCT LIABILITY
- 350 MOTOR VEHICLE
- 355 MOTOR VEHICLE PRODUCT LIABILITY
- 360 OTHER PERSONAL INJURY
- 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- 365 PERSONAL INJURY - PRODUCT LIABILITY
- 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK

- 370 OTHER FRAUD
- 371 TRUTH IN LENDING
- 380 OTHER PERSONAL PROPERTY DAMAGE
- 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK

- 422 APPEAL 28 USC 158
- 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK

- 440 OTHER CIVIL RIGHTS
- 441 VOTING
- 442 EMPLOYMENT
- 443 HOUSING/ ACCOMMODATIONS
- 445 AMERICANS with DISABILITIES - Employment
- 446 AMERICANS with DISABILITIES - Other
- 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK

- 462 NATURALIZATION APPLICATION
- 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK

- 463 HABEAS CORPUS- Alien Detainee
- 510 MOTIONS TO VACATE SENTENCE
- 530 HABEAS CORPUS
- 535 HABEAS CORPUS DEATH PENALTY
- 540 MANDAMUS & OTHER
- 550 CIVIL RIGHTS - Filed Pro se
- 555 PRISON CONDITION(S) - Filed Pro se
- 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK

- 550 CIVIL RIGHTS - Filed by Counsel
- 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK

- 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK

- 710 FAIR LABOR STANDARDS ACT
- 720 LABOR/MGMT. RELATIONS
- 740 RAILWAY LABOR ACT
- 751 FAMILY and MEDICAL LEAVE ACT
- 790 OTHER LABOR LITIGATION
- 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK

- 820 COPYRIGHTS
- 840 TRADEMARK
- 880 DEFEND TRADE SECRETS ACT OF 2016 (DTSA)

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK

- 830 PATENT
- 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (ANDA) - a/k/a Hatch-Waxman cases

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK

- 861 HIA (1395f)
- 862 BLACK LUNG (923)
- 863 DIWC (405(g))
- 863 DIWW (405(g))
- 864 SSID TITLE XVI
- 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK

- 870 TAXES (U.S. Plaintiff or Defendant)
- 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK

- 375 FALSE CLAIMS ACT
- 376 Qui Tam 31 USC 3729(a)
- 400 STATE REAPPORTIONMENT
- 430 BANKS AND BANKING
- 450 COMMERCE/ICC RATES/ETC.
- 460 DEPORTATION
- 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- 480 CONSUMER CREDIT
- 485 TELEPHONE CONSUMER PROTECTION ACT
- 490 CABLE/SATELLITE TV
- 890 OTHER STATUTORY ACTIONS
- 891 AGRICULTURAL ACTS
- 893 ENVIRONMENTAL MATTERS
- 895 FREEDOM OF INFORMATION ACT 899
- 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK

- 410 ANTI TRUST
- 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK

- 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23 DEMAND \$ >\$5,000,000
 JURY DEMAND YES NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE _____ DOCKET NO. _____

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)

- 1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- 2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- 3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- 4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.
- 5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.
- 6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):

7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. _____, WHICH WAS DISMISSED. This case IS IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.


 SIGNATURE OF ATTORNEY OF RECORD

June 5, 2023
 DATE

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Middle District of Georgia

Emily Ramos, an individual, on behalf of herself
and all others similarly situated,

Plaintiff(s)

v.

Mercer University

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address)

Mercer University
c/o Matthew R Hall, Registered Agent
1501 Mercer University Drive
Macon, GA 31207

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

G. Franklin Lemond, Jr.
Webb, Klase & Lemond, LLC
1900 The Exchange SE, Suite 480
Atlanta, GA 30339

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: 06/05/2023

Signature of Clerk or Deputy Clerk

Civil Action No. _____

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____
was received by me on *(date)* _____ .

I personally served the summons on the individual at *(place)* _____
_____ on *(date)* _____ ; or

I left the summons at the individual's residence or usual place of abode with *(name)* _____
_____, a person of suitable age and discretion who resides there,
on *(date)* _____ , and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* _____ , who is
designated by law to accept service of process on behalf of *(name of organization)* _____
_____ on *(date)* _____ ; or

I returned the summons unexecuted because _____ ; or

Other *(specify)*: _____

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ _____ 0.00 _____ .

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc: