SALTZ MONGELUZZI & BENDESKY P.C.
BY: PATRICK HOWARD
IDENTIFICATION NO: 88572
1650 MARKET STREET
52ND FLOOR
PHILADELPHIA, PENNSYLVANIA 19103
(215) 496-8282
Additional counsel on signature page

ATTORNEYS FOR PLAINTIFFS

BLAKE BOJE 4617 McCreary Road Erie, PA 16506, Individually and on Behalf of All Others Similarly Situated, *Plaintiff* vs. **MERCYHURST UNIVERSITY,** 501 E 38th Street, Erie, PA 16546 *Defendant*	**ERIE COUNTY** **COURT OF COMMON PLEAS** **LAW DIVISION** **No.:** 10041-2023 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Blake Boje ("Plaintiff") bring this action on behalf of himself, and all others similarly situated against Defendant, Mercyhurst University, ("Mercyhurst" or "Defendant"), and alleges as follows:

SUMMARY OF THE CASE

1. Defendant Mercyhurst, a private Pennsylvania university, lost control over its employees', students', and former students' highly sensitive personal information in a data breach by cybercriminals ("Data Breach"). The number of total breach victims is unknown, but on information and belief, the Data Breach has impacted at least thousands of students, former students, and other persons associated with the University.

2. According to Mercyhurst's Data Breach notice, (the "Breach Notice," attached as **Ex. A)**[1] the Data Breach occurred between January 16 and May 15, 2022. As a result of an investigation that was completed on September 16, 2022, Defendant's investigations revealed that cybercriminals gained unauthorized access to current and former employees' personally identifiable information ("PII") stored on Defendant's network.

3. On information and belief, cybercriminals bypassed Defendant's inadequate security systems to access employees' and students' PII in Defendant's computer systems.

4. On information and belief, the stolen PII included, at least, names, Social Security numbers, and financial account information.

5. On or around November 8, 2022—almost a year after the Data Breach first occurred—Defendant finally began notifying victims about the breach.

6. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell the victims how many people were impacted, how the breach happened, or why it took the Defendant nearly a year to begin notifying victims that hackers had gained access to highly sensitive employee information.

7. Defendant's failure to timely detect and report the Data Breach made its current and former employees and students vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

---

[1] A true and accurate copy of Defendant's Breach Noticed is attached to this Complaint as **Exhibit A**. Breach Notice obtained from the website of the office of the Massachusetts Attorney General, https://www.mass.gov/doc/assigned-data-breach-number-28542-mercyhurst-university/download (last visited December 13, 2022).

9. In failing to adequately protect employees' and students' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its current and former employees and students.

10. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff Boje is a former Mercyhurst student and Data Breach victim. Mr. Boje was a student at Mercyhurst from 2011 to 2015 and graduated from Mercyhurst in 2015.

12. Accordingly, Plaintiff, on his own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff Blake Boje is a natural person and citizen of Pennsylvania, residing in Erie, Pennsylvania, where he intends to remain. Mr. Boje is a graduate of Mercyhurst University and Data Breach victim, receiving Defendant's Breach Notice on or about November 8, 2022.

14. Plaintiff Boje has taken great steps to protect his sensitive personal information, including using credit monitoring services and has locked his credit so no additional fraudulent transactions can take place.

15. Defendant Mercyhurst University is a Pennsylvania Non-Profit Corporation, with its principal place of business at 501 E. 38th Street, Erie, Pennsylvania, 16504. Defendant is a private, Roman Catholic University, with approximately 2500 students and more than 500

employees at any time.

JURISDICTION & VENUE

16. This Court has jurisdiction over this action because Plaintiff and at least two-thirds (2/3) of the proposed class of Plaintiffs and Defendant are citizens of the Commonwealth of Pennsylvania and further because both Plaintiff and Defendant reside in Erie County.

17. Venue is proper in this Court because both Plaintiff and Defendant reside in Erie County and because the events relevant to Plaintiff's cause of action occurred in Erie County.

BACKGROUND FACTS

a. Mercyhurst

18. Mercyhurst University is a private, Roman Catholic university. According to the U.S. Department of Education, Mercyhurst currently has 3,041 students, of which 2,641 are undergraduates.

19. Mercyhurst is the home of the Ridge College of Intelligence Studies & Applied Sciences, which provides an undergraduate program in cyber security, as well as graduate programs in cyber security and cyber risk management.[2]

20. As part of its educational mission, Defendant collects and maintains PII on its students. Students are obligated to provide this information to Defendant in order to enroll in school at Defendant's institution.

21. In fact, shortly before the Data Breach occurred, Defendant participated in, and presented at, a Department of Defense event discussing cybersecurity attacks on key infrastructure.[3]

---

[2] https://www.mercyhurst.edu/stories/cyber-attacks-escalate-mercyhurst-stands-ready (last accessed December 13, 2022).

[3] https://www.mercyhurst.edu/news/ridge-college-joins-dod-sanctioned-large-scale-cyberattack-exercise (last visited Dec. 14, 2022).

22. On information and belief, Defendant maintains former students' PII for years—even decades—after the student graduates or no longer enrolls.

23. Additionally, Defendant collects and maintains the PII of its employees, including teaching and administrative staff.

24. On information and belief, Defendant maintains former employees' PII for years, including after those individuals are no longer employed by Defendant.

25. Despite recognizing its duty to do so—as demonstrated by its dedicated cyber security program—on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect employee and student PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves vulnerabilities in its systems for cybercriminals to exploit and gain access to employee and student PII.

b. Defenant Fails to Safeguard Employee and Student PII

26. As a condition of enrollment in school, Defendant requires its students to disclose their names and Social Security numbers, as well as financial information related to student aid and tuition payment.

27. As a condition of employment with Defendant, Defendant requires its employees to disclose their names and Social Security numbers, as well as financial account information.

28. On information and belief, Defendant collects and maintains student and employee PII in its computer systems.

29. In collecting and maintaining the PII, Defendant implicitly agrees it will safeguard the data using reasonable means according to its internal policies and federal law.

30. According to the November 2022, Breach Notice, Defendant "discovered

suspicious activity in its environment" "[e]arlier this year." Ex. A.

31. Defendant's investigation "determined that an unauthorized actor had the ability to access certain information stored on the network" "between January 16, 2022 and May 15, 2022." *Id.*

32. On information and belief, this data breach was perpetrated by the well-known cybercriminal group "LockBit," which published online its intent to release the information stolen in the Data Breach if Defendant failed to pay the requested ransom by May 22, 2022.[4]

33. On information and belief, Defendant did in fact pay a ransom to LockBit in exchange for it agreeing not to publish the stolen data.[5]

34. According to Defendant, its internal investigation was completed on September 16, 2022, despite all facts pointing to it having paid a ransom for the stolen data on or before May 22, 2022. But affected individuals were not notified until November. No explanation was given for this delay.

35. Plaintiff and the Class place value in data privacy and security. Plaintiff and the Class would not have gone to school at Defendant's institution or accepted employment with Defendant, nor provided their PII, to Defendant had they known that Defendant does not take all necessary precautions to secure the personal and financial data given to it by its students and employees.

36. Despite its duties and alleged commitments to safeguard PII, Defendant does not follow industry standard practices in securing students' and employees' PII, as evidenced by the Data Breach and stolen student and employee PII.

[4] https://www.suspectfile.com/erie-us-pa-mercyhurst-university-ransomware-attack/ (last accessed Dec. 14, 2022)/
[5] https://www.suspectfile.com/lockbit-cancels-mercyhurst-university-from-its-website-ransom-paid/ (last accessed Dec. 14, 2022).

37. In response to the Data Breach, Defendant contends that it "took steps to implement additional safeguards and review our policies and procedures relating to data privacy and security." Exh. A. Although Defendant fails to expand on these alleged "additional safeguards," such steps should have been in place *before* the Data Breach.

38. Through its Breach Notice, Mercyhurst also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Exh. A.

39. On information and belief, Defendant has offered only twelve months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers. Further, the breach exposed students' and employees' nonpublic financial information, a disturbing harm in and of itself.

40. Even with complimentary credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

41. On information and belief, Defendant failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over employee PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that Defendant cannot, or will not, determine the full scope of the Data Breach, as it has been unable to determine exactly what information was stolen and when.

Plaintiff Boje

42. Plaintiff is a former student of Defendant Mercyhurst University. He was enrolled from 2011 to 2015 and graduated from Mercyhurst in May 2015.

43. As a condition of enrolling, Plaintiff was required to provide his PII to Defendant.

44. Plaintiff provided his PII to Defendant and trusted that it would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

45. Plaintiff received a Breach Notice on or about November 8, 2022, from Defendant indicating that his PII, including at least his name, financial account number, and Social Security number, may have been compromised in the Data Breach.

46. In addition to the damages detailed herein, the Data Breach has caused Plaintiff to be at substantial risk for further identity theft.

47. Plaintiff has taken great steps to protect his sensitive personal information, including signing up for credit monitoring, not transmitting his personal information via un-encrypted means, regularly monitoring his credit reports, and locking his credit cards.

48. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

c. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

49. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

50. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII

secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, or other nonpublic financial information, without permission, to commit fraud or other crimes.

51. The types of personal data compromised and potentially stolen in the Data Breach is highly valuable to identity thieves. The stolen PII can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

52. Identity thieves can also use this data to harm Plaintiff and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

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

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended 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;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

54. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[6]

55. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

56. It can take victims years to spot identity or PII theft, giving criminals plenty of time

[6] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited July 7, 2022).

to use that information for cash.

57. One such example of criminals using PII for profit is the development of "Fullz" packages.

58. 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. These dossiers are known as "Fullz" packages.[7]

59. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's 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 stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

60. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity

[7] *Id.*

fraud), all using the stolen PII.

61. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and members of the proposed Class to unscrupulous operators, con artists, and criminals.

62. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

d. Mercyhurst Failed to Adhere to FTC Guidelines

63. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

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

a. protect the personal customer information that they keep;

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

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

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

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

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

68. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

e. Plaintiff and Class Members Suffered Damages

69. The compromised and stolen information of Plaintiff and Class members is private and sensitive in nature and was left inadequately protected by Defendant. Defendant did not obtain Plaintiff's and Class members' consent to disclose this data to any other person as required by applicable law and industry standards.

70. As discussed above, Plaintiff's personal, private, and sensitive data, including but not limited to financial data, which Defendant allowed to be stolen has already been used to inflict

harm on Plaintiff.

71. The data breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff's and Class members' personal data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including the failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' sensitive personal information to protect against reasonably foreseeable threats to the security or integrity of such information.

72. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and the Class Members' confidential personal, sensitive, and private information and data.

73. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting data breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

74. Defendant's wrongful actions and inaction directly and proximately caused the

potential theft and dissemination into the public domain of Plaintiff's and Class members' personal data, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the actual, imminent, and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed in the hands of criminals and misused via the sale of Plaintiff's and Class members' information on the Internet's black market;

d. the untimely and inadequate notification of the data breach;

e. the improper disclosure of their personal data;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach;

h. ascertainable losses in the form of deprivation of the value of their personal data, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the data breach;

j. loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their

credit including adverse credit notations; and

k. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data breach

CLASS ACTION ALLEGATIONS

75. Plaintiff brings this action pursuant to Pennsylvania Rule of Civil Procedure 1702 on behalf of himself and all members of the proposed class (the "Class"), defined as follows:

> **Class:** All individuals residing in the United States whose personal information was compromised in the Data Breach disclosed by Mercyhurst University in November 2022.

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

77. Plaintiff reserves the right to amend the Class definition or add a Class if further information and discovery indicate that other classes should be added and if the definition of the Class should be narrowed, expanded, or otherwise modified.

78. **Numerosity**. The exact number of Class members is unknown but is estimated to be up to thousands of former and current Mercyhurst employees and students at this time, and individual joinder in this case is impracticable. Class Members can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, unlawful trade practices, and class action controversies

79. In view of the complexities of the issues and the anticipated expenses of this litigation, the separate claims of individual Class Members are insufficient in amount to support separate actions.

80. **Commonality**. There are many questions of law and fact common to the claims of Plaintiff and the Class. Common questions for the Class include, but are not necessarily limited to the following:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

ii. 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;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

v. Whether Defendant publicized Plaintiff's and the Class's private life;

vi. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vii. Whether Defendant's Breach Notice was reasonable;

viii. Whether the Data Breach caused Plaintiff and the Class injuries;

ix. What the proper damages measure is; and

x. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

81. **Typicality:** Plaintiff's claims are typical of the claims of the other members of their respective classes because, among other things, Plaintiff and the other Class members were injured through the substantially uniform misconduct by Defendant. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

82. Prosecution of separate actions by or against individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class members which would confront the party opposing the class with incompatible standards of conduct.

83. Prosecution of separate actions by or against individual Class Members would create a risk of adjudications with respect to individual Class Members which would as a practical matter be dispositive of the interests of other Class Members not parties to the adjudications or substantially impair or impede their ability to protect their interests.

84. **Adequacy of Representation:** Plaintiff is an adequate representative of the classes because their interests do not conflict with the interests of the other Class members they seek to represent; he has retained counsel competent and experienced in complex class action litigation and Plaintiff will prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiff and their counsel

85. **Superiority and Predominance:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other members of their respective classes are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

86. To Plaintiff's knowledge, there are no other pending actions by or against the Plaintiff or the Class Members involving any of the same issues germane to this action

87. This forum is appropriate for the litigation of the claims for all Class Members because Defendant Mercyhurst University is located and headquartered in this forum and the alleged harm and Defendant's liability-inducing conduct occurred in this forum.

88. The questions of law and fact common to the Class Members predominate over any questions of law or fact that may affect only individual members. Defendant unlawfully permitted unauthorized access to and receipt of the Class Members personal, private, and sensitive information, which has resulted in damages to Plaintiff and the Class.

CLAIMS ALLEGED ON BEHALF OF PLAINTIFF AND THE CLASS

First Claim for Relief
Negligence
(On Behalf of Plaintiff and the Class)

89. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

90. Plaintiff and members of the Class entrusted their PII to Defendant. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their personal data and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the personal data of Plaintiff's and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

91. Mercyhurst was under a basic duty to act with reasonable care when it undertook to collect, create, and store Plaintiff's and the Class's sensitive data on its computer system, fully aware–as any reasonable entity of its size would be–of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the

criminal acts of a third party.

92. Defendant knew that the personal data of Plaintiff and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the personal data of Plaintiff and the Class was wrongfully disclosed, that disclosure was not fixed.

93. By being entrusted by Plaintiff and the Class to safeguard their personal data, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class agreed to provide their personal data with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

94. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' personal data by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite failures and intrusions, and allowing unauthorized access to Plaintiff's and the other Class member's personal data.

95. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their personal data would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the personal data of Plaintiff and the Class and all resulting damages.

96. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' personal data. Defendant knew its systems and technologies for processing and securing the personal data of Plaintiff and the Class had numerous security vulnerabilities.

97. As a result of this misconduct by Defendant, the personal data of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their personal data was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their personal data in that it is now easily available to hackers on the Dark Web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Second Claim for Relief
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

98. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

99. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

100. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, students' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's sensitive PII.

101. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect personal data and not complying with applicable industry standards, as described in detail herein.

102. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*

103. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

104. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

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

106. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

107. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

108. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

109. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their personal data, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Mercyhurst fails to undertake appropriate and adequate measures to protect their personal data in its continued possession.

Third Claim for Relief
Breach of Confidence
(On Behalf of Plaintiff and the Class)

110. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

111. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' personal data that Plaintiff and Class Members provided to Defendant.

112. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' personal data would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

113. Plaintiff and Class Members provided their respective personal data to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the personal data to be disseminated to any unauthorized parties.

114. Plaintiff and Class Members also provided their respective personal data to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that personal data from unauthorized disclosure, such as following basic principles of information security practices.

115. Defendant voluntarily received in confidence Plaintiff's and Class Members' personal data with the understanding that the personal data would not be disclosed or disseminated to the public or any unauthorized third parties.

116. Due to Defendant's failure to prevent, detect, and/or avoid the data breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class Members' personal data, Plaintiff's and Class Members' personal data was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

117. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

118. But for Defendant's disclosure of Plaintiff's and Class Members' personal data in violation of the parties' understanding of confidence, their personal data would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data breach was thedirect and legal cause of the theft of Plaintiff's and Class Members' personal data, as well as the resulting damages.

119. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' personal data. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' personal data had numerous security vulnerabilities because Defendant failed to observe industry standard information security practices.

120. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the data

breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

121. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

Fourth Claim for Relief
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

122. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

123. Plaintiff and the Class entrusted their PII to Defendant at the time they enrolled in school with Defendant or accepted employment from Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

124. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant by either paying Defendant tuition or by providing Defendant with their employment services, which were facilitated by their transmission of their PII to Defendant.

125. Defendant breached the implied contracts it made with Plaintiff and the Class by

failing to adequately safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

126. Had Plaintiff and the Class known that Defendant would not reasonably protect their PII, they would not have entered into relationships with Defendant and would not have provided Defendant with their PII.

127. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

128. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

Fifth Claim for Relief
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

129. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

130. This claim is pleaded in the alternative to the breach of implied contractual duty

claim.

131. Plaintiff and Class Members conferred a monetary benefit on Defendant by paying tuition and other fees to Defendant.

132. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and by retaining the benefit of Plaintiff's and the Class's tuition and fees and/or employment services.

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

134. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

135. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

136. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

137. Plaintiff and Class Members have no adequate remedy at law.

138. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft

of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

139. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

140. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

Sixth Claim for Relief
Publicity Given to Private Life
(On Behalf of Plaintiff and the Class)

141. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

142. One who gives publicity to matters concerning the private life of another, of a kind highly offensive to a reasonable man, is subject to liability to the other for invasion of his privacy.

143. As a condition of enrolling as a student or obtaining employment with Defendant, Plaintiff and the Class provided Defendant with sensitive personal information, including names,

Social Security numbers, and financial account information.

144. Defendant failed to employ adequate and reasonable security measures to prevent public disclosure of Plaintiff's and the Class's private information.

145. Defendant failed to timely and reasonably notify Plaintiff and the Class about the data breach for a period of months, which made Plaintiff and the Class vulnerable to identify theft.

146. As a result of the disclosure of Plaintiff's and the Class's private information, Plaintiff and the Class have suffered a de facto injury, which entitles them to general damages.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

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

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

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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

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

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

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

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: January 9, 2023 By:

Patrick Howard; ID No. 88572
1650 Market Street, 52nd Floor
Philadelphia, PA 19103
Tel: (215) 496-8282
phoward@smbb.com

Matthew R. Wilson*
Michael J. Boyle, Jr.*
MEYER WILSON CO., LPA
305 W. Nationwide Blvd.
Columbus, OH, 43215
Telephone: (614) 224-6000
mwilson@meyerwilson.com
mboyle@meyerwilson.com

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

Attorneys for Plaintiffs and the putative class

**Pro hac vice* motions to be filed

ClassAction.org
