UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS
NORTHERN DIVISION

KELLY SHEA, on behalf of herself and all others similarly situated, Plaintiff, v. AMERICAN INTERNATIONAL COLLEGE, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Kelly Shea ("Plaintiff"), on behalf of herself and all others similarly situated, states as follows for her class action complaint against Defendant, AMERICAN INTERNATIONAL COLLEGE ("AIC" or "Defendant"):

INTRODUCTION

1. On December 15, 2023, AIC, a private university headquartered in Springfield, Massachusetts, lost control over its computer network and the highly sensitive personal information stored on its computer network in a data breach perpetrated by cybercriminals ("Data Breach"). Upon information and belief, the Data Breach has impacted at least 11,000 current and former students.

2. On information and belief, the Data Breach occurred between November 14, 2023, and December 3, 2023. However, Defendant did not become aware of the Breach until December 3, 2024, allowing cybercriminals unfettered access to its systems for over *nineteen* days.

3. Following an internal investigation, Defendant learned cybercriminals had gained unauthorized access to students' personally identifiable information ("PII"), including but not limited to names and Social Security numbers.

4. On or about May 8, 2024–six after the Data Breach first occurred– AIC finally began notifying Class Members about the Data Breach ("Breach Notice"). A sample Breach Notice to Maine residents is attached as Exhibit A.

5. Upon information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII—rendering it an easy target for cybercriminals.

6. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its students how many people were impacted, how the breach happened, or why it took the Defendant almost six months to finally begin notifying victims that cybercriminals had gained access to their highly private information.

7. Defendant's failure to timely report the Data Breach made the victims 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.

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

10. Plaintiff and the 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 is a former student and Data Breach victim.

12. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

PARTIES

13. Plaintiff, Kelly Shea, is a natural person and citizen of Massachusetts, where she intends to remain.

14. Defendant, American International College, is incorporated in Massachusetts, with its principal place of business at 170 Wilbraham Road, Springfield, Massachusetts.

JURISDICTION & VENUE

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are over 100 putative Class Members.

16. This Court has personal jurisdiction over Defendant because it is headquartered in Massachusetts, and regularly conducts business in Massachusetts. At least one class member and Defendant are from different states.

17. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

AIC

18. AIC is a private university located in Springfield, Massachusetts that offers both

undergraduate and graduate programs.[1] AIC boasts an annual revenue of $134.6 million.[2]

19. On information and belief, AIC accumulates highly private PII of its current and former students.

20. In collecting and maintaining its students' PII, Defendant agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

21. AIC understood the need to protect its current and former students' PII and prioritize its data security.

22. Indeed, AIC states in its Privacy Policy that it does not **"**sell, trade, or otherwise transfer to outside parties your Personally Identifiable Information unless we provide users with advance notice."[3]

23. AIC further assures its students that it "is committed to ensuring that your privacy is protected."[4]

24. Despite recognizing its duty to do so, on information and belief, AIC has not implemented reasonably cybersecurity safeguards or policies to protect student's PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, AIC leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to students' PII.

AIC Fails to Safeguard Students' PII

25. Plaintiff is a former student of AIC.

---

[1] AIC, About us, https://www.aic.edu/about/ (last visited June 3, 2024).
[2] Zoominfo, American International College, https://www.zoominfo.com/c/american-international-college/7443658 (last visited June 3, 2024).
[3] AIC, Privacy Policy, https://www.aic.edu/privacy-policy/ (last visited June 3, 2024).
[4] *Id*.

26. As a condition of employment with AIC, Plaintiff provided Defendant with her PII, including but not limited to her name and Social Security Number. Defendant used that PII to facilitate its enrollment of Plaintiff and required Plaintiff to provide that PII to enroll as a student.

27. On information and belief, AIC collects and maintains students' unencrypted PII in its computer systems.

28. In collecting and maintaining PII, Defendant implicitly agreed that it will safeguard the data using reasonable means according to state and federal law.

29. According to the Breach Notice, AIC admits that "[o]n December 3, 2023, AIC discovered suspicious activity in its environment." Ex A. An internal investigation revealed that the Breach had began as early as November 14, 2023, and lasted until at least December 3, 2023, without discovery, meaning cybercriminals had unfettered access to students' most sensitive information for at least *nineteen* days before detection.

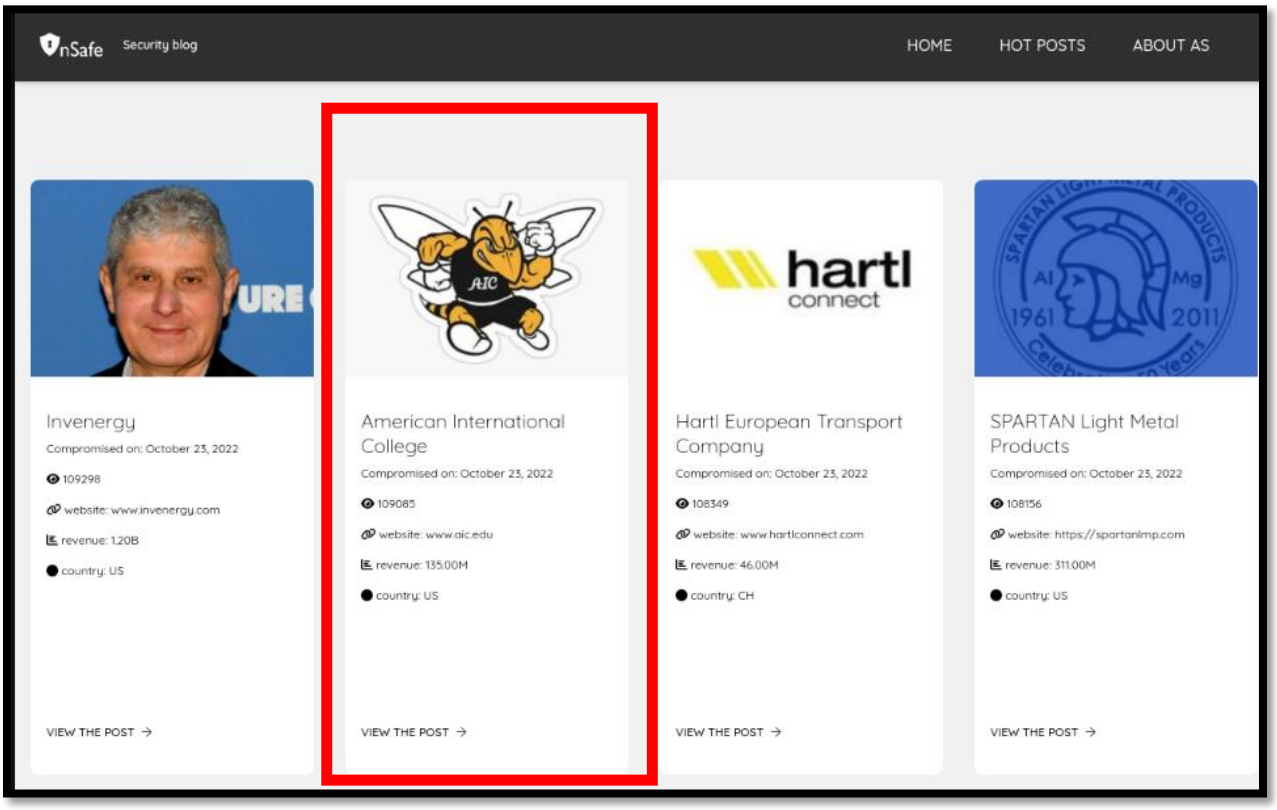
30. Further, as a result of the Data Breach, the "unauthorized actor had the ability to access or take certain information stored on the network during this period of time." Ex. A. In other words, the Data Breach investigation revealed Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its students' highly private information.

31. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

32. On information and belief, the nSafe ransomware gang, a newer cyber-hacking group quickly gaining notoriety within the cybercriminal sphere, claimed responsibility for the cyberattack. With a logged 102 confirmed ransomware attacks on the United States education sector in 2023 alone, AIC knew or should have known of the tactics that cybercriminals groups

like nSafe employ.

33. With the PII secured and stolen by nSafe, the hackers then purportedly issued a ransom demand to AIC. However, AIC has provided no public information on the ransom demand or payment.



34. On or about May 8, 2024–six months after the Data Breach occurred– AIC finally began notifying some Class Members about the Data Breach.

35. Despite its duties to safeguard PII, Defendant did not in fact follow industry standard practices in securing students' PII, as evidenced by the Data Breach.

36. In response to the Data Breach, AIC contends that it "took steps to implement additional safeguards and review [its] policies and procedures relating to data privacy and security." Ex. A. Defendant not only fails to expand on what these "reviews" are, but also fails to identify what steps, if any, have been taken as a result of this Data Breach. Further, these "steps"

and any additional modifications made as a result of its review, should have been in place before the Data Breach.

37. Through its Breach Notice, Defendant 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." Ex. A

38. Through the Data Breach, Defendant recognized its duty to implement reasonable cybersecurity safeguards or policies to protect students' PII, insisting that, despite the Data Breach demonstrating otherwise, it "takes the confidentiality, privacy, and security of information in its care seriously." Ex. A.

39. On information and belief, AIC has offered several 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, due to Defendant's failure to provide adequate notice, some victims, including Plaintiff, are unable to access the credit monitoring offered by Defendant.

40. Even with several months of 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. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

42. On information and belief, AIC 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 its students' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of Which Defendant was on Notice.

43. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

44. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[5]

45. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), AIC knew or should have known that its electronic records would be targeted by cybercriminals.

46. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

47. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

---

[5] Data breaches break record in 2021, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed September 4, 2023).

48. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

49. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[6]

50. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[7]

51. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[8]

---

[6] High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI, available at https://www.ic3.gov/Media/Y2019/PSA191002 (last accessed September 4, 2023).

[7] Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet, https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed September 4, 2023).

[8] Ransomware Guide, U.S. CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last accessed September 4, 2023).

52. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

53. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of thousands of its current and former students in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

54. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

55. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its students' Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Plaintiff's Experience and Injuries

56. Plaintiff Kelly Shea a former student of Defendant and a data breach victim.

57. As a condition of enrolling, AIC required Ms. Shea to provide her PII, including at least her name and Social Security Number in order to enroll as a student.

58. Ms. Shea provided her PII to AIC and trusted that the company would use reasonable measures to protect it according to state and federal law.

59. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about the Breach for six months.

60. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

61. Plaintiff does not recall ever learning that her PII was compromised in a data breach incident, other than the breach at issue in this case.

62. Plaintiff suffered actual injury from the exposure of her PII —which violates her rights to privacy.

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

64. As a result of the Data Breach, Plaintiff has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, placing a credit freeze through all the three main credit bureaus, and monitoring Plaintiff's credit information.

65. Plaintiff has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her 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. Plaintiff is experiencing anxiety, distress, and fear regarding how this Data Breach, including the exposure and loss of her Social Security number, will impact her ability to do so. 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.

66. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties, including the cybercriminal group nSafe. This injury was worsened by Defendant's failure to inform Plaintiff about the Data Breach in a timely fashion.

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

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

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

69. As a result of AIC'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. Plaintiff and the class 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 its possession.

70. 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.

71. 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.

72. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

73. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

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

75. 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.

76. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the 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 the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and members of the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

77. 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 the 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 fraud), all using the stolen PII.

78. Defendant's failure to properly notify Plaintiff and the Class of the Data Breach exacerbated Plaintiff's and the Class's injuries 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.

Defendant failed to adhere to FTC guidelines.

79. 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.

80. 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.

81. 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.

82. 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.

83. 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.

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

Defendant Failed to Follow Industry Standards

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

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

87. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

causing the Data Breach.

CLASS ACTION ALLEGATIONS

89. Plaintiff is suing on behalf of herself and the proposed Class ("Class"), defined as follows:

> **All individuals residing in the United States whose PII was compromised in Defendant's Data Breach, including all those who received notice of the breach.**

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

91. Plaintiff reserves the right to amend the class definition.

92. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff's claim is representative of the proposed Class, consisting of at least 11,000 individuals, far too many to join in a single action;

b. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claim is typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interest does not conflict with Class members' interests, and Plaintiff has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

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 took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

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

f. **Appropriateness**. The likelihood that individual members of the Class will prosecute separate actions is remote due to the time and expense necessary to prosecute an individual case. Plaintiff is not aware of any litigation concerning this controversy already commenced by others who meet the criteria for class membership described above.

g. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Class)

93. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

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

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

96. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

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

98. Defendant owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect

the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII.

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

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

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

102. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of employment from Defendant.

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

104. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff's and Class Members' and the importance of exercising reasonable care in handling it.

105. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

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

107. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

108. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff's and Class Members' injury.

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

110. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

111. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary

damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

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

SECOND CLAIM FOR RELIEF
Negligence *per se*
(On Behalf of Plaintiff and the Class)

113. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

114. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

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

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

117. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as

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

118. 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.

119. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and Class Members would not have been injured.

120. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their 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.

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

122. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*)

THIRD CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

123. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

124. Defendant offered to employ Plaintiff and members of the Class if, as a condition of that employment, Plaintiff and members of the Class provided Defendant with their PII.

125. In turn, Defendant agreed it would not disclose the PII it collects to unauthorized

persons. Defendant also promised to safeguard student's PII.

126. Plaintiff and the members of the Class accepted Defendant's offer by providing PII to Defendant in exchange for enrollment with Defendant.

127. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

128. Plaintiff and the members of the Class would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

129. Defendant materially breached the contracts it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

130. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

131. Plaintiff and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

132. The covenant of good faith and fair dealing is an element of every contract. All

such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

134. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

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

136. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

137. Plaintiff, on behalf of herself and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of the Plaintiff and the Class)

138. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

139. This claim is plead in the alternative to the breach of implied contractual duty claim.

140. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of services through employment. Defendant also benefited from the receipt of Plaintiff's and the

Class's PII, as this was used to facilitate their employment.

141. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

142. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the proposed Class's services and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII or worked for Defendant at the payrates they did had they known Defendant would not adequately protect their PII.

143. Defendant should be compelled to disgorge into a common fund to benefit Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

FIFTH CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of the Plaintiff and the Class)

144. Plaintiff incorporates all previous paragraphs as if fully set forth herein.

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

146. Defendant owed a duty to its students, including Plaintiff and the Class, to keep this information confidential.

147. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

148. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant as part of their employment, but they did so privately, with the intention that their information would be

kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

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

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

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

153. As a proximate result of Defendant's acts and omissions, the PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

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

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

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

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 her 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 DEMAND

Plaintiff hereby demands that this matter be tried before a jury.

Dated: June 4, 2024,

Respectfully Submitted,

/s/ *Anthony Paronich*

Anthony Paronich
PARONICH LAW, P.C.
350 Lincoln Street, Suite 2400
Hingham, Massachusetts 02043
Telephone: (617) 485-0018
Facsimile: (508) 318-8100
anthony@paronichlaw.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borelli (*Pro Hac Vice* forthcoming)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
(872) 263-1109 (facsimile)
sam@straussborrelli.com
raina@straussborrelli.com

* *Pro hac vice forthcoming*

Attorneys for Plaintiff and Proposed Class