UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SANTOSH CHERIAN, on behalf of himself and all others similarly situated, Plaintiff, v. **MANIPAL EDUCATION AMERICAS, LLC,** and **AMERICAN UNIVERSITY OF ANTIGUA INC.**, Defendants.	No. 24-cv-404 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Santosh Cherian ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendants Manipal Education Americas, LLC, and American University of Antigua Inc. ("AUA" or "Defendants"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendants' failure to protect highly sensitive data.

2. Defendants operate and/or constitute the American University of Antigua College of Medicine—which is a for-profit private medical school based in the Caribbean.[1]

3. As such, Defendants stores a litany of highly sensitive personal identifiable information ("PII") about its current and former students. But Defendants lost control over that

[1] *Why AUA*, AMERICAN UNIV. ANTIGUA, https://www.auamed.org/why-aua/facts-and-figures/ (last visited Jan. 16, 2024).

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

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

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

6. Plaintiff is a Data Breach victim, having received a breach notice—attached as Exhibit A. He brings this class action on behalf of himself, and all others harmed by Defendants' misconduct.

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

PARTIES

8. Plaintiff, Santosh Cherian, is natural person and citizen of Georgia. He resides in Warner Robins, Georgia where he intends to remain.

9. Defendant, Manipal Education Americas, LLC, is a Limited Liability Company incorporated in New York and with its principal place of business at 40 Wall Street, 10th Floor, New York, New York 10005.

10. Defendant, American University of Antigua Inc., is a Private Ordinary Company with its principal place of business at University Park, Jabberwock Beach Road, Coolidge, Antigua.

JURISDICTION AND VENUE

11. 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. Plaintiff and Defendants are citizens of different states. And there are over 100 putative Class members.

12. This Court has personal jurisdiction over Defendants because they are headquartered in New York, regularly conduct business in New York, and/or have sufficient minimum contacts in New York.

13. Venue is proper in this Court because Defendants' 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.

BACKGROUND

Defendants Collected and Stored the PII of Plaintiff and the Class

14. Defendants operate and/or constitute the American University of Antigua College of Medicine—which is a for-profit private medical school based in the Caribbean.[2]

15. American University of Antigua Inc. is owned and operated by Manipal Education Americas, LLC.[3] Specifically, Defendants state that "American University of Antigua is a

[2] *Why AUA*, AMERICAN UNIV. ANTIGUA, https://www.auamed.org/why-aua/facts-and-figures/ (last visited Jan. 16, 2024).
[3] *Academic Catalog 2023*, AMERICAN UNIV. ANTIGUA, https://www.auamed.org/wp-content/uploads/2023/03/AUA-Academic-Catalog-SPRING-2023.pdf (last visited Jan. 16, 2024).

corporation duly authorized and existing under the laws of Antigua and Barbuda" and that "[i]t is owned and operated by Manipal Education Americas, LLC, a New York limited liability company."

16. As part of its business, Defendants receives and maintains the PII of thousands of its current and former students.

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

18. Under state and federal law, businesses like Defendants have duties to protect its current and former students' PII and to notify them about breaches.

19. Defendants recognizes these duties, declaring in its "Student Handbook" that:

a. "American University of Antigua respects its students' right to privacy and confidentiality of personally identifiable information (PII)."[4]

20. And via its ""Privacy Policy," Defendants declare that:

a. "Your privacy is important to us."[5]

b. "It is American University of Antigua's policy to respect your privacy and comply with any applicable law and regulation regarding any personal information we may collect about you[.]"[6]

---

[4] *Student Handbook*, AMERICAN UNIV. ANTIGUA, https://www.auamed.org/wp-content/uploads/2022/01/AUACOM_Spring_2022_Student_Handbook.pdf (last visited Jan. 16, 2024).
[5] *Privacy Policy*, AMERICAN UNIV. ANTIGUA, https://www.auamed.org/privacy-policy/ (last visited Jan. 16, 2024).
[6] *Id*.

c. "We only collect and use your personal information when we have a legitimate reason for doing so. In which instance, we only collect personal information that is reasonably necessary to provide our services to you."[7]

d. "We keep your personal information only for as long as we need to."[8]

e. "If your personal information is no longer required for this purpose, we will delete it or make it anonymous by removing all details that identify you."[9]

f. "The personal information we collect is stored and/or processed in United States, or where we or our partners, affiliates, and third-party providers maintain facilities."[10]

g. "When we collect and process personal information, and while we retain this information, we will protect it within commercially acceptable means to prevent loss and theft, as well as unauthorized access, disclosure, copying, use, or modification."[11]

h. "We will comply with laws applicable to us in respect of any data breach."[12]

Defendants' Data Breach

21. From August 30, 2023, until September 6, 2023, Defendants were hacked.[13]

---

[7] *Id*.
[8] *Id*.
[9] *Id*.
[10] *Id*.
[11] *Id*.
[12] *Id*.
[13] *Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/7f1348b0-8ffa-45ef-afc5-170379df5567.shtml (last visited Jan. 16, 2024).

22. Worryingly, Defendants already admitted that "an unauthorized actor *accessed* and *acquired* certain files from computer systems on its network."[14]

23. Because of Defendants' Data Breach, at least the following types of PII were compromised:

a. names;

b. Social Security numbers;

c. driver's license numbers;

d. government ID numbers;

e. passport numbers;

f. state ID numbers;

g. financial information;

h. financial account numbers;

i. credit card numbers;

j. debit card numbers; and

k. financial account security codes, access codes, passwords, and PINs.[15]

24. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendants' custody and control. And upon information and belief, the putative class is over one hundred members—as it includes its current and former students.

---

[14] *Id*. (emphasis added).

[15] *Data Security Breach Reports*, ATTY GEN. TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Jan. 16, 2024); *Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/7f1348b0-8ffa-45ef-afc5-170379df5567.shtml (last visited Jan. 16, 2024).

25. And yet, Defendants waited over until November 15, 2023, before it began notifying the class—a full 77 days after the Data Breach began.[16]

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

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

a. "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity;"

b. "obtain information" from "the Federal Trade Commission and/or the Attorney General's office in your state" about "steps an individual can take to avoid identity theft as well as information;" and

c. "refer to www.ExperianIDWorks.com/restoration for . . . additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s)."[17]

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

---

[16] *Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/7f1348b0-8ffa-45ef-afc5-170379df5567.shtml (last visited Jan. 16, 2024).

[17] *Id*.

29. Since the breach, Defendants have "taken steps to enhance our existing security measures."[18] But this is too little too late. Simply put, these measures—which Defendants now recognizes as necessary—should have been implemented *before* the Data Breach.

30. On information and belief, Defendants failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

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

32. Defendants have done little to remedy its Data Breach. True, Defendants have offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class members for the injuries that Defendants inflicted upon them.

33. Because of Defendants' Data Breach, the sensitive PII of Plaintiff and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class members.

34. Worryingly, the cybercriminals that obtained Plaintiff's and Class members' PII appear to be the notorious cybercriminal group "ALPHV Blackcat."[19] Thus far, reports indicate that:

a. "The hackers uploaded 16 attachments of documents allegedly from the American University of Antigua cyber attack."[20]

---

[18] *Id*.
[19] Vishwa Pandagle, *ALPHV Ransomware Strikes American University of Antigua, Leaves Detailed Ransom Note*, CYBER EXPRESS (Sept. 20, 2023) https://thecyberexpress.com/american-university-of-antigua-cyber-attack/.
[20] *Id*.

b. "The officials of AUA were threatened by the ALPHV ransomware group with multiple warnings in an attempt to extort money."[21]

c. "The hackers from ALPHV ransomware group also known as the BlackCat claimed that they gained access to the AUA systems and continued investigating the data for a long time."[22]

35. And screenshots of ALPHV's dark web website include digital scans of several individuals' *passports*.[23]

36. Furthermore, those screenshots include ALPHV's ransom demand which states:

a. "Our team has been in your institute's network for a long time."[24]

b. "We have obtained all the most interesting data, internal documentation, a complete list of your students' documents and much more."[25]

37. ALPHV Blackcat is an especially notorious cybercriminal group. In fact, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint report warning the public about ALPHV Blackcat.[26] Specifically, the joint "Cybersecurity Advisory" (CSA) stated, *inter alia*, that:

---

[21] *Id*.
[22] *Id*.
[23] *Alphv*, RANSOMLOOK, https://www.ransomlook.io/screenshots/alphv/American%20University%20of%20Antigua.png (last visited Jan. 16, 2024).
[24] *Id*.
[25] *Id*.
[26] *ALPHV Blackcat*, FBI & CISA (Dec. 19, 2023) https://www.cisa.gov/sites/default/files/2023-12/aa23-353a-stopransomware-alphv-blackcat_0.pdf.

a. "ALPHV Blackcat actors released a new version of the malware, and the FBI identified over 1000 victims worldwide targeted via ransomware and/or data extortion."[27]

b. "This ALPHV Blackcat update has the capability to encrypt both Windows and Linux devices, and VMWare instances."[28]

c. "ALPHV Blackcat affiliates have extensive networks and experience with ransomware and data extortion operations."[29]

d. "According to the FBI, as of September 2023, ALPHV Blackcat affiliates have compromised over 1000 entities—nearly 75 percent of which are in the United States and approximately 250 outside the United States—, demanded over $500 million, and received nearly $300 million in ransom payments."[30]

e. "ALPHV Blackcat affiliates use advanced social engineering techniques and open source research on a company to gain initial access."[31]

f. "Some ALPHV Blackcat affiliates exfiltrate data after gaining access and extort victims without deploying ransomware. After exfiltrating and/or encrypting data, ALPHV Blackcat affiliates communicate with victims via TOR, Tox, email, or encrypted applications."[32]

---

[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*

38. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[33]

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

Plaintiff's Experiences and Injuries

40. Plaintiff Santosh Cherian is a former student of Defendants—having been a student from approximately 2017 until 2023.

41. Thus, Defendants obtained and maintained Plaintiff's PII.

42. As a result, Plaintiff was injured by Defendants' Data Breach.

43. As a condition of receiving educational services, Plaintiff provided Defendants with his PII. Defendants used that PII to facilitate its provision of educational services and to collect payment.

44. Plaintiff provided his PII to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

45. Plaintiff reasonably understood that a portion of the funds paid to Defendants would be used to pay for adequate cybersecurity and protection of PII.

46. Plaintiff received a Notice of Data Breach dated November 15, 2023.

---

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

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

48. Through its Data Breach, Defendants compromised Plaintiff's:

a. name;

b. Social Security number;

c. driver's license number;

d. financial account number; and

e. passport number.

49. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendants directed Plaintiff to take those steps in its breach notice.

50. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam phone calls—with the spike beginning in or around September 2023 (which precisely dovetails with the timing of the Data Breach).

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

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

53. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

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

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

56. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

57. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

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

58. Because of Defendants' failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

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

b. diminution in value of their PII;

c. compromise and continuing publication of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII; and

h. continued risk to their PII—which remains in Defendants' possession—and is thus as risk for futures breaches so long as Defendants fails to take appropriate measures to protect the PII.

59. 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.

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

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

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

63. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

64. 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 Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

65. Defendants disclosed the PII of Plaintiff and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PII of Plaintiff and Class members 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.

66. Defendants' failure to promptly and properly notify Plaintiff and Class members of the Data Breach exacerbated Plaintiff and Class members' 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.

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

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

68. In 2021, a record 1,862 data breaches occurred, exposing approximately

293,927,708 sensitive records—a 68% increase from 2020.[34]

69. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[35]

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

Defendants Failed to Follow FTC Guidelines

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

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[36] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

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

---

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

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

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

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

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

74. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

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

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

Defendants Failed to Follow Industry Standards

77. 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.

78. 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.

79. Defendants 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.

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

CLASS ACTION ALLEGATIONS

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

> All individuals residing in the United States whose PII was compromised in the Data Breach discovered by Defendants in or

> around September 2023, including all those individuals who received notice of the breach.

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

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

84. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

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

86. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least 100 members.

87. Typicality. Plaintiff's claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

88. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

89. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting

individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

b. if Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendants were negligent in maintaining, protecting, and securing PII;

d. if Defendants breached contract promises to safeguard Plaintiff and the Class's PII;

e. if Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendants' Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

90. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendants would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties

and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

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

91. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

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

93. Defendants owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendants' 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.

94. Defendants have 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.

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

96. Defendants 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.

97. Thus, Defendants 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.

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

99. Defendants 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.

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

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

102. 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 Defendants' duty to protect Plaintiff and the Class members' sensitive PII.

103. Defendants 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. Defendants' conduct was particularly unreasonable given the nature and amount of PII Defendants 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.

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

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

106. Defendants 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.

107. Defendants breached these duties as evidenced by the Data Breach.

108. Defendants 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.

109. Defendants breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

110. Defendants 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 and Class members' injuries-in-fact.

111. Defendants have admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

112. As a direct and traceable result of Defendants' 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.

113. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

114. Defendants' 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 Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

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

115. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

116. Plaintiff and Class members were required to provide their PII to Defendants as a condition of receiving educational services provided by Defendant. Plaintiff and Class members provided their PII to Defendants or its third-party agents in exchange for Defendants' educational services.

117. Plaintiff and Class members reasonably understood that a portion of the funds they paid Defendants would be used to pay for adequate cybersecurity measures.

118. Plaintiff and Class members reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendants' duties under state and federal law and its internal policies.

119. Plaintiff and the Class members accepted Defendants' offers by disclosing their PII to Defendants or its third-party agents in exchange for educational services.

120. In turn, and through internal policies, Defendants agreed to protect and not disclose the PII to unauthorized persons.

121. In its Privacy Policy, Defendants represented that they had a legal duty to protect Plaintiff's and Class Member's PII.

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

123. After all, Plaintiff and Class members would not have entrusted their PII to Defendants in the absence of such an agreement with Defendant.

124. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

125. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

127. Defendants materially breached the contracts it entered with Plaintiff and Class members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendants created, received, maintained, and transmitted.

128. In these and other ways, Defendants violated its duty of good faith and fair dealing.

129. Defendants' material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed *supra*).

130. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

131. Plaintiff and Class members performed as required under the relevant agreements, or such performance was waived by Defendants' conduct.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

132. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

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

134. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendants benefitted from using their PII to provide educational services and to collect payment.

135. Defendants appreciated or had knowledge of the benefits it received from Plaintiff and Class members.

136. Plaintiff and Class members reasonably understood that Defendants would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendants' duties under state and federal law and its internal policies.

137. Defendants enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII.

138. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendants 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 Defendants' failure to provide the requisite security.

139. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's and Class members' PII and/or payment because Defendants failed to adequately protect their PII.

140. Plaintiff and Class members have no adequate remedy at law.

141. Defendants should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

142. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

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

144. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendants' relationship with them—especially to secure their PII.

145. Because of the highly sensitive nature of the PII, Plaintiff and Class members would not have entrusted Defendant, or anyone in Defendants' position, to retain their PII had they known the reality of Defendants' inadequate data security practices.

146. Defendants breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII.

147. Defendants also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

148. As a direct and proximate result of Defendants' breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

FIFTH CAUSE OF ACTION
Violation of New York Deceptive Trade Practices Act ("GBL")
New York Gen. Bus. Law § 349
(On Behalf of Plaintiff and the Class)

149. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

150. Under the New York Gen. Bus. Law § 349, "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

151. Notably, Defendants' deceptive acts and/or practices were directed at consumers. After all, via its "Privacy Policy" and "Student Handbook," Defendants represented to consumers that they would, *inter alia*, use reasonably adequate data security.

152. And these deceptive acts—including the quotations provided *supra*—were materially misleading insofar as they induced consumers to rely on such statements and disclose their PII.

153. Section § 349 applies to Defendants because there is a sufficient nexus between Defendants' conduct and New York. After all, Manipal Education Americas, LLC, is incorporated in New York and its corporate headquarters is in New York, New York.

154. And, upon information and belief, the misleading acts and/or practices alleged herein—including the manifestations in Defendants' "Privacy Policy" and "Student Handbook"—were written, approved, and/or otherwise authorized by Defendants within the state of New York.

155. In particular, Defendants violated Section § 349 by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

156. Defendants' omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of their PII.

157. Defendants intended to mislead Plaintiff and Class members and induce them to rely on its omissions.

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

159. Defendants acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiff's and Class members' rights.

160. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury,

ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

161. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

162. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law.

SIXTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

163. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

164. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

165. In the fallout of the Data Breach, an actual controversy has arisen about Defendants' various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendants' actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

166. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendants have a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendants breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendants breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

167. The Court should also issue corresponding injunctive relief requiring Defendants to use adequate security consistent with industry standards to protect the data entrusted to it.

168. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendants experiences a second data breach.

169. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class members' injuries.

170. If an injunction is not issued, the resulting hardship to Plaintiff and Class members far exceeds the minimal hardship that Defendants could experience if an injunction is issued.

171. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class members, and the public at large.

PRAYER FOR RELIEF

Plaintiff and Class members respectfully request judgment against Defendants and 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 necessary to protect the interests of Plaintiff and the Class;

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

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

E. Awarding Plaintiff and the Class damages including 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 other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: January 18, 2024

Respectfully submitted,

By: /s/ James J. Bilsborrow
James J. Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
Telephone: (212) 558-5500
jbilsborrow@weitzlux.com

TURKE & STRAUSS LLP
Samuel J. Strauss (BAR #/PRO HAC VICE)
Raina Borrelli (BAR #/PRO HAC VICE)
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiff and Proposed Class