IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

JENNIE DEVRIES, individually and on behalf of all others similarly situated, Plaintiff, v. HOPE COLLEGE, Defendant.	Case No: **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jennie Devries ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint and alleges the following against Defendant Hope College ("Hope College" or "Defendant"), based upon personal knowledge with respect to Plaintiff and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE ACTION

1. This class action arises out of the recent data breach (the "Data Breach") involving Hope College, which collected and stored certain personally identifiable information ("PII") of the Plaintiff and the putative Class Members, all of whom have PII on Hope College servers.

2. According to Hope College, the PII that was subject to "unauthorized access" in the Data Breach included highly-sensitive information: first and last names, date of birth, Social Security numbers, driver's license numbers, and student ID numbers.[1]

[1] Exhibit A, Hope College Press Release (Dec. 15, 2022), *Notice of Data Security Event*, available at https://hope.edu/_resources/cybersecurityupdate.pdf (last accessed Dec. 26, 2022).

3. Social Security numbers are particularly valuable to criminals. This information can be sold and traded on the dark web black market. The loss of a Social Security number is particularly troubling because it cannot be easily changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

4. The Data Breach was a direct result of Hope College's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII. Hope College itself has acknowledged that it first discovered the cybersecurity attack on or around September 27, 2022, but it has only recently begun contacting Class Members.

5. According to the Office of the Maine Attorney General, whom Hope College was required to notify, the Data Breach has affected 156,783 individuals.[2]

6. Plaintiff brings this class action lawsuit individually as well as on behalf of all those similarly situated to address Hope College's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was unsecured and left open to the unauthorized access of any unknown third party.

PARTIES

7. Plaintiff Jennie Devries is an adult individual and citizen of the State of Michigan who resides in Holland, Michigan.

8. On or around December 15, 2022, Plaintiff was notified by Defendant via letter of the Data Breach and of the impact to her PII.

[2] Exhibit B, Office of the Maine Attorney General (Dec. 2022), *Data Breach Notifications* https://apps.web.maine.gov/online/aeviewer/ME/40/9574bf0a-94d2-4653-8665-da79a7728b4b.shtml (last accessed Dec. 26, 2022).

9. As a result of Hope College's failure to adequately protect the sensitive information entrusted to it, Plaintiff suffered actual damages including, without limitation, time and expenses related to monitoring their financial accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of her personal information, and other economic and non-economic harm. Plaintiff and Class Members will now be forced to expend additional time to review their credit reports and monitor their financial accounts and medical records for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

10. Defendant Hope College is a private Christian liberal arts college in Holland, Michigan, with its principal place of business at 141 E 12th Street, Holland, Michigan 49423.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this controversy pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendant's state of citizenship.

12. This Court has personal jurisdiction over Hope College because it is authorized to and does conduct substantial business in this District, and is a citizen of this District by virtue of its principal place of business being located in this District.

13. Venue is proper under 28 U.S.C. §1391(b) because the cause of action upon which the complaint is based arose in Holland, Michigan, which is in the Western District of Michigan.

COMMON FACTUAL ALLEGATIONS

14. Plaintiff and the proposed Class have all entrusted their sensitive personal information to Defendant, a private Christian liberal arts college in Holland, Michigan.[3]

15. As noted above, Plaintiff brings this class action against Hope College for its failure to properly secure and safeguard personally identifiable information, for failing to comply with industry standards to protect and safeguard that information, and for failing to provide timely and adequate notice to Plaintiff and other members of the class that such information had been compromised.

Hope College's Unsecure Data Management and Disclosure of Data Breach

16. Plaintiff and Class Members provided their PII to Hope College with the reasonable expectation and mutual understanding that it would comply with its obligations to keep such information confidential and secure from unauthorized access.

17. Plaintiff and Class Members' PII was provided to Defendant in conjunction with the type of work Defendant performs as an educational institution.[4]

18. However, Defendant failed to secure the PII of the individuals that provided it with this sensitive information.

19. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date it disclosed the incident.

---

[3] Exhibit C, Hope College Webpage, *About* section (as of Dec. 26, 2022) https://hope.edu/about/index.html (last accessed Dec. 26, 2022).

[4] *Id*.

20. According to Hope College, "potential unauthorized access to its network" was discovered on September 27, 2022.[5] Hope College said that it "undertook a comprehensive review process to identify what personal information, if any, was present within the potentially impacted files, and to whom that information belonged."[6] In addition, it consulted with its own IT team as well as "third party forensic and legal specialists" to assist its investigation, but notably omitted from its notice any change to its data security or retention policies.[7]

21. Despite being aware of the breach on September 27, 2022, Defendant failed to take any action to notify Plaintiff or other class members of this breach until at least December 15, 2022.

22. Defendant failed to take appropriate or even the most basic steps to protect the PII of Plaintiff and other class members from being disclosed.

Plaintiff and the Class Have Suffered Injury as a Result of Defendant's Data Mismanagement

23. As a result of Defendant's failure to implement and follow even the most basic security procedures, Plaintiff's and Class Members' PII has been and is now in the hands of unauthorized individuals, which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiff and other Class Members now face an increased risk of identity theft, particularly due to the dissemination of their Social Security Number, and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to Defendant's Data Breach.

[5] *See* Exhibit A, *supra*.

[6] *Id.*

[7] *Id.*

24. Plaintiff and other class members have had their most personal, sensitive and PII disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

25. Plaintiff and class members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk for falling victim for cybercrimes for years to come.

26. PII is a valuable property right.[8] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[9] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[10] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

27. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and

[8] *See* Exhibit D, Marc van Lieshout, *The Value of Personal Data* at p. 4, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 10, 2015), available at https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible[.]") (last visited Dec. 26, 2022).

[9] Exhibit E, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economic Papers No. 220 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited Dec. 26, 2022).

[10] Exhibit F, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited Dec. 26, 2022).

other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

28. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

29. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[14]

30. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[11] Exhibit G, Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Dec. 26, 2022).

[12] Exhibit H, Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Dec. 26, 2022).

[13] Exhibit I, *In the Dark*, VPNOverview.com, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on Dec. 26, 2022).

[14] Exhibit J, Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1 (last visited Dec. 26, 2022).

31. 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 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.[15]

32. Plaintiff and members of the Class, as a whole, must immediately devote time, energy, and money to: 1) closely monitor their bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

33. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct. Further, the value of Plaintiff's and Class members' PII has been diminished by its exposure in the Data Breach.

34. As a result of Defendant's failures, Plaintiff and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their PII.

35. Plaintiff and the Class suffered actual injury from having PII compromised as a result of Defendant's negligent data management and resulting Data Breach including, but not

[15] Exhibit K, 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 (last visited December 26, 2022).

limited to (a) damage to and diminution in the value of their PII, a form of property that Defendant obtained from Plaintiff; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

36. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and members of the Class these significant injuries and harm.

37. Plaintiff brings this class action against Defendant for Defendant's failure to properly secure and safeguard PII and for failing to provide timely, accurate, and adequate notice to Plaintiff and other class members that their PII had been compromised.

38. Plaintiff, individually and on behalf of all other similarly situated individuals, alleges claims in negligence, negligence per se, breach of implied contract, breach of fiduciary duty, unjust enrichment, and violation of the Michigan Consumer Protection Act.

CLASS ACTION ALLEGATIONS

39. Plaintiff brings this action individually and on behalf of all other persons similarly situated pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

40. Plaintiff proposes the following Nationwide Class and Michigan Subclass definition (collectively "Class"), subject to amendment as appropriate:

Nationwide Class

All persons whose PII was compromised in the Data Breach that was discovered by Hope College on or around September 27, 2022.

Michigan Subclass

All residents of Michigan whose PII was compromised in the Data breach that was discovered by Hope College on or around September 27, 2022.

41. Excluded from the Classes are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Classes are

Members of the judiciary to whom this case is assigned, their families and Members of their staff.

42. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Classes meet the criteria for certification under Rule 23(a), 23(b)(2), 23(b)(3), and 23(c)(4).

43. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. As noted above, there are approximately 156,783 Members.

44. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. 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;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether computer hackers obtained Class Members' PII in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Defendant's conduct was negligent;

j. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

k. Whether Defendant's acts breaching an implied contract they formed with Plaintiff and the Class Members;

l. Whether Defendant violated the Federal Trade Commission Act ("FTC Act");

m. Whether Defendant was unjustly enriched to the detriment of Plaintiff and the Class;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

o. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

45. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

46. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

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

48. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively

high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

49. Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

50. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant's data security practices were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

51. Finally, all members of the proposed Classes are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. At least some

Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Michigan Subclass)

71. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

72. Hope College owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

73. Hope College knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class members' PII and the importance of maintaining secure systems. Hope College knew, or should have known, of the vast uptick in data breaches in recent years. Hope College had a duty to protect the PII of Plaintiff and Class Members.

74. Given the nature of Hope College's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, Hope College should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which Hope College had a duty to prevent.

75. Wing breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class members' PII.

76. It was reasonably foreseeable to Hope College that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

77. But for Hope College's negligent conduct/breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

78. As a result of Hope College's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, the Michigan Subclass)

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. Hope College's duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Hope College, of failing to employ reasonable measures to protect and secure PII.

81. Hope College violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class members' PII and not complying with applicable industry standards. Hope College's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

82. Hope College's violations of Section 5 of the FTCA constitutes negligence per se.

83. Plaintiff and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

84. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against.

85. It was reasonably foreseeable to Hope College that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

86. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Hope College's violations of Section 5 of the FTCA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and

actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Michigan Subclass)

87. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

88. Plaintiff and Class members either directly or indirectly gave Hope College their PII in confidence, believing that Hope College – a private college – would protect that information. Plaintiff and Class members would not have provided Hope College with this information had they known it would not be adequately protected. Hope College's acceptance and storage of Plaintiff's and Class members' PII created a fiduciary relationship between Hope College and Plaintiff and Class Members. In light of this relationship, Hope College must act primarily for the benefit of its customers and students, which includes safeguarding and protecting Plaintiff's and Class Members' PII.

89. Hope College has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII, failing

to comply with the data security guidelines set forth by Section 5 of the FTCA, and otherwise failing to safeguard the PII of Plaintiff and Class Members it collected.

90. As a direct and proximate result of Hope College's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Hope College's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Michigan Subclass)

91. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein. This claim is pled in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d)(2).

92. Plaintiff and Class Members conferred a monetary benefit upon Hope College in the form of monies paid for educational services or other services.

93. Hope College accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Hope College also benefitted from the receipt of Plaintiff's and Class Members' PII.

94. As a result of Hope College's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with

reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

95. Hope College should not be permitted to retain the money belonging to Plaintiff and Class Members because Hope College failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

96. Hope College should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Michigan Subclass)

97. Plaintiff realleges and incorporates by reference all allegations of the preceding factual allegations as though fully set forth herein.

98. Defendant required Plaintiff and Class Members to provide, or authorize the transfer of, their PII in order for Hope College to provide services. In exchange, Hope College entered into implied contracts with Plaintiff and Class Members in which Hope College agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

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

100. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

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

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

COUNT VI
VIOLATION OF THE MICHIGAN CONSUMER PROTECTION ACT
(Mich. Comp. Laws Ann § 445.90, *et. seq.*)
(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the Michigan Subclass)

103. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

104. The Michigan Consumer Protection Act was created to protect Michigan consumers from unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce.

105. Plaintiff and Class members provided PII to Defendant pursuant to transactions (i.e., providing education) they engaged in with Defendant as customers and students.

106. Defendant has its principal place of business and headquarters in Michigan and transacts with Michigan consumers and students.

107. Hope College engaged in deceptive trade practices in the conduct of its business, in violation of Mich. Comp. Laws Ann § 445.901, including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

108. Hope College's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff 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 and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and COPPA, 15 U.S.C. §§ 6501-6505, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and COPPA, 15 U.S.C. §§ 6501-6505;

f. Failing to timely and adequately notify Plaintiff, and class members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class Members' PII; and

h. 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 and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and COPPA, 15 U.S.C. §§ 6501-6505.

109. Hope College's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Hope College's data security and ability to protect the confidentiality of consumers' PII.

110. Hope College's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and the Class members, that their PII was not exposed and misled Plaintiff and the Class members into believing they did not need to take actions to secure their identities.

111. Hope College intended to mislead Plaintiff and Class members and induce them to rely on its misrepresentations and omissions.

112. Had Hope College disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Hope College 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. Instead, Hope College was trusted with sensitive and valuable PII regarding hundreds of thousands of consumers, including Plaintiff, and the Michigan Subclass. Hope College accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Hope College held itself out as maintaining a secure platform for PII data, Plaintiff and the Class members acted reasonably in relying on Hope College's misrepresentations and omissions, the truth of which they could not have discovered.

113. As a direct and proximate result of Hope College's deceptive trade 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.

114. Class members are likely to be damaged by Hope College's ongoing deceptive trade practices.

115. Plaintiff and the Class members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive or other equitable relief, and attorneys' fees and costs.

116. Accordingly, pursuant to Mich. Comp. Law Ann. § 445.901, *et seq.*, Michigan Plaintiffs and Class members are entitled to recover their actual damages, which can be calculated with a reasonable degree of certainty using sufficiently definitive and objective evidence. Those damages are: (a) damage to and diminution in the value of their PII, a form of property that Defendant obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; (c) present and increased risk arising from the identity theft and fraud.; and other miscellaneous incidental and consequential damages. In addition, given the nature of Hope College's conduct, Michigan Plaintiffs and Class members are entitled to all available statutory, exemplary, treble, and/or punitive damages and attorneys' fees based on the amount of time reasonably expended and equitable relief necessary or proper to protect them from Hope College's unlawful conduct.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class and Subclass;

b. For equitable relief enjoining Hope College from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data

Breach;

d. For an order requiring Defendant to pay for an appropriate period of time's worth of credit monitoring services for Plaintiff and the Class;

e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

f. For an award of punitive damages, as allowable by law;

g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h. Pre and post-judgment interest on any amounts awarded; and

i. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: December 26, 2022

Respectfully Submitted By:
THE MILLER LAW FIRM, P.C.

/s/ E. Powell Miller
E. Powell Miller (P39487)
Sharon S. Almonrode (P33938)
Emily E. Hughes (P68724)
950 W. University Dr., Suite 300
Rochester, MI 48307
T: (248) 841-2200
epm@millerlawpc.com
ssa@millerlawpc.com
eeh@millerlawpc.com

SHUB LAW FIRM LLC
Jonathan Shub*
Benjamin F. Johns*
134 Kings Hwy E., Fl. 2,
Haddonfield, NJ 08033
T: (856) 772-7200
F: (856) 210-9088
jshub@shublawyers.com
bjohns@shublawyers.com

Attorneys for Plaintiff and the Proposed Class

**Pro Hac Vice Forthcoming*