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

IN RE HOPE COLLEGE DATA SECURITY BREACH LITIGATION	Case No: 1:22-cv-01224-PLM **CONSOLIDATED [CLASS] ACTION** **JURY TRIAL DEMANDED**

CONSOLIDATED AMENDED COMPLAINT

Plaintiffs Jennie Devries, Tricia Garnett, Mark Cyphers, Timothy Drost, and Joseph Rodgers, Emily Damaska, and Elise Carter (collectively "Plaintiffs"), individually and on behalf of all others similarly situated, bring this class action against Defendant Hope College ("Defendant" or "Hope College"). Plaintiffs seek to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Hope College for its failure to adequately safeguard the sensitive information entrusted to it. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

INTRODUCTION

1. This class action arises out of the 2022 data breach (referred to herein as the "Data Breach") on Hope College's network that resulted in unauthorized access to highly sensitive personally identifiable information of approximately 156,783 individuals. As a result, Plaintiffs and Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to

remedy or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their sensitive personal information.

2. Hope College is a private liberal arts college located in Holland, Michigan. It currently enrolls approximately 3,200 students and hosts a variety of on-campus events for students and non-students alike.

3. According to Hope College, the highly sensitive personally identifiable information that was subject to "unauthorized access" in the Data Breach included: first and last names, date of birth, Social Security numbers, driver's license numbers, and student ID numbers (collectively "PII").

4. 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 credit and identity theft.

5. 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 Data Breach on or around September 27, 2022, but it has only recently begun contacting Class Members starting on December 15, 2022.

6. According to Hope College's posted Notice of Data Security Event on its website[1], as well as the Notice Letters[2] it sent Attorneys General and some Class Members,

[1] **Exhibit A**, Hope College Press Release (Dec. 15, 2022), Notice of Data Security Event, available via The Wayback Machine at:

Hope College provided scant detail, particularly considering the size and scope of the Data Breach and the sensitivity of Plaintiffs' and Class Members' compromised information.

7. Hope College's Notice of Data Security Event states, in relevant part, that it "discovered potential unauthorized access to its network" on or around September 27, 2022. It went on to state that it "immediately began working with its IT team and third-party forensic and legal specialists were engaged to conduct a full forensic investigation." As a result of the investigation, Hope College reports that "certain sensitive information kept in the normal course of business may have been subject to unauthorized use" including "individuals' first and last names, in combination with date of birth, Social Security number, driver's license number, and Student ID number."

8. Neither Hope College's Notice of Data Security Event nor its Notice Letter disclosed how it discovered the unauthorized access, the means and mechanisms of the unauthorized access, the reason for its nearly four month delay in notifying Plaintiffs and the Class of the Data Breach after learning that their PII was impacted, how Hope College determined that the PII was "subject to unauthorized access," and, importantly, what steps Hope College took following the Data Breach to secure its systems and prevent future unauthorized access.

---

https://web.archive.org/web/20230111195758if_/https://hope.edu/_resources/cybersecurityupdate.pdf (last visited Mar. 16, 2023).

[2] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/9574bf0a-94d2-4653-8665-da79a7728b4b/7a50da1a-1609-4b27-af7b-ab04401d29a6/document.html (last visited Mar. 16, 2023). (the "Notice Letter" or "Notice Letters") (**Exhibit B** hereto).

9. According to the Office of the Maine Attorney General, who Hope College was required to notify, the Data Breach affected approximately 156,713 individuals.[3]

10. The Data Breach was a direct result of Hope College's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect individuals' PII from the foreseeable thread of a cyberattack.

11. By taking possession and control of Plaintiffs' and Class Members' PII for its own benefit, Hope College assumed a duty to Plaintiffs and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiffs' and Class Members' PII against unauthorized access and disclosure. Hope College also had a duty to adequately safeguard this PII under industry standards and duties imposed by operation of law, including by Section 5 of the Federal Trade Commission Act ("FTC Act"). Hope College breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII of Plaintiffs and Class Members from unauthorized access and disclosure.

12. The exposure of a person's PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. As a result of the Data Breach, Plaintiffs and Class Members are at imminent and substantial risk of experiencing various types of misuse of their PII in the coming years, including but not limited to, unauthorized access to personal accounts, tax fraud, and identity theft.

---

[3] https://apps.web.maine.gov/online/aeviewer/ME/40/9574bf0a-94d2-4653-8665-da79a7728b4b.shtml (last visited Mr. 16, 2023) (**Exhibit C** hereto).

13. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures.

14. As a result of Hope College's inadequate security and breach of its duties and obligations, the Data Breach occurred, Plaintiffs and over 156,000 Class Members, suffered injury and ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminution in value of their personal information from its exposure, emotional distress, and the present and imminent risk of fraud and identity theft caused by the compromise of their sensitive personal information. Plaintiffs' and Class Members' sensitive PII—which was entrusted to Hope College, its officials, and its agents—was compromised and unlawfully accessed due to the Data Breach.

15. The security of Plaintiffs' and Class Members' identities is now at risk because of Hope College's wrongful conduct as the PII that Hope College collected and maintained is now in the hands of data thieves. This present risk will continue for the course of their lives.

16. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to actual fraud and identity theft as well as a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against further fraud and identity theft.

17. Plaintiffs and Class Members may also incur out-of-pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

18. Plaintiffs and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts for fraud or identity theft. Due to the fact that the exposed information potentially includes Social Security numbers ("SSNs") and other immutable personal details, Plaintiffs and Class Members will be at risk of identity theft and fraud that will persist throughout the rest of their lives.

19. Plaintiffs bring this Class Action Complaint for Defendant's failure to comply with industry standards to protect their information systems that contain PII and Defendant's failure to provide timely and adequate notice to Plaintiffs and other Class Members that their PII had been compromised.

20. Plaintiffs, individually and all others similarly situated, bring claims for negligence; negligence *per se*; breach of fiduciary duty; unjust enrichment; breach of implied contract; violation of the Michigan Consumer Protection Act, Mich. Comp. Laws Ann § 445.901, *et. seq.*; and injunctive relief claims.

21. Plaintiffs seek, among other things, damages and injunctive relief requiring Defendant to fully and accurately disclose the PII and other information that has been compromised; to adopt reasonably sufficient security practices and safeguards to protect Plaintiffs' and Class Members' PII from unauthorized disclosures in order to prevent incidents like the Data Breach from reoccurring in the future, and to safeguard the PII that remains in Defendant's custody.

22. Plaintiffs further seek an order requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide free credit monitoring and identity theft insurance to all Class Members for ten (10) years, as Plaintiffs and Class Members are at risk and will continue to be at an increased risk

of identity theft due to the unauthorized disclosure of their PII as a result of Hope College's conduct described herein.

PARTIES

A. Plaintiffs

23. Plaintiff Jennie Devries is a resident and citizen of the State of Michigan. Plaintiff Devries sent her ACT scores to Hope College around March of 2011, and subsequently received a notice letter from Hope College on or around December 20, 2022, informing her that her PII was impacted by the Data Breach.

24. Plaintiff Tricia Garnett is a resident and citizen of the State of Arizona. In 2007, Plaintiff Garnett applied to attend Hope College as a student and provided Hope College with her PII on her application. In December 2022, Plaintiff received a notice letter from Hope College informing her that her PII was impacted by the Data Breach.

25. Plaintiff Mark Cyphers is a resident and citizen of the State of Michigan. Plaintiff Cyphers performed work for Hope College as a contractor, and as a condition of this working relationship, he provided Hope College with his PII.

26. Plaintiff Timothy Drost is a resident and citizen of the State of Michigan. Plaintiff Drost is an employee of Hope College, and as a condition of his employment, he provided Hope College with his PII. Plaintiff Drost subsequently received a notice letter from Hope College in December 2022, informing him that his PII was impacted by the Data Breach.

27. Plaintiff Joseph Rodgers is a resident and citizen of the State of Indiana. Plaintiff Rodgers attended a football game at Hope College approximately 30 years ago, and subsequently received a notice letter from Hope College on or around December 15, 2022, informing him that his PII was impacted by the Data Breach.

28. Plaintiff Emily Damaska is a resident and citizen of the State of Michigan. Plaintiff Damaska attended Hope College as a student from 2016 to 2020, and she provided Hope College with her PII in order to attend the college and receive an education. In December 2022, Plaintiff Damaska received a notice letter from Hope College informing her that her PII was impacted by the Data Breach.

29. Plaintiff Elise Carter is a resident and citizen of the State of Michigan. Around 2018, Plaintiff Carter applied to attend Hope College as a student and provided Hope College with her PII on her application. In December 2022, Plaintiff Carter received a notice letter from Hope College informing her that her PII was impacted by the Data Breach.

B. Defendant

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

31. Hope College was entrusted with and in possession of Plaintiffs' PII.

JURISDICTION AND VENUE

32. 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.

33. 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.

Venue is proper in this District, pursuant to 28 U.S.C. § 1391(b), because a substantial part of the acts, omissions, and events giving rise to Plaintiffs' claims occurred in Holland, Michigan, which is in this District.

FACTUAL ALLEGATIONS

A. Background

34. Defendant Hope College is a private liberal arts college. There are only approximately 3,251 students currently enrolled at Hope College. Yet, Hope College has inexplicably collected, stored, and failed to protect the highly sensitive PII of over more than 156,000 individuals.

35. In its Notice Letters, Hope College claims that it "take[s] the privacy and security of the information in [its] care seriously, and sincerely regret[s] any worry or inconvenience this incident may cause…"

36. Plaintiff and the Class Members, as current or former students, applicants, employees, contractors, or attendants of events at Hope College, reasonably relied (directly or indirectly) on this sophisticated higher education institution to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. People demand security to safeguard their PII, especially when Social Security numbers are involved as here.

37. Hope College had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties and as evidenced by the Data Breach, it failed to adhere to that duty.

38. Plaintiffs 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.

39. Plaintiffs and Class Members' PII was provided to Hope College in conjunction with the type of work Hope College performs as an educational institution and/or a host of public events.

40. However, Hope College failed to secure the PII of the individuals that provided it with this sensitive information.

41. Hope College'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.

B. The Data Breach and Notice Letter

42. In Hope College's December 15, 2022, Notice Letter to Plaintiffs and Class Members, as well as in its Notice of Data Security Incident posted to their website (since removed), Hope College announced that on or around September 27, 2022, Hope College discovered "unauthorized access" to its network and engaged third-party specialists to conduct a forensic investigation.

43. Hope College's investigation determined that certain sensitive information kept in the normal course of business was subject to this "unauthorized access."

44. Hope College stated that the "information believed to be at risk includes individuals' first and last names, in combination with date of birth, Social Security number, driver's license number, and Student ID number."

45. Once Hope College discovered that certain files may have been accessed by an "unauthorized party," Hope College undertook a review process to identify what personal information was present. Hope College completed that review on November 8, 2022.

46. Plaintiffs' PII including Social Security numbers, were part of the data acquired by the "unauthorized party" from Hope College's systems in the Data Breach.

47. Despite being aware of the Data Breach on September 27, 2022, Hope College failed to take any action to notify Plaintiffs or other Class Members of this breach until at least December 15, 2022.

48. Hope College failed to take appropriate or even the most basic steps to protect the PII of Plaintiffs and other Class Members from being disclosed.

49. In addition, Hope College consulted with their own "IT team" as well as "third party forensic and legal specialists" to assist its "investigation." Additional items of PII as well as other facts surrounding the Data Breach may be uncovered or have already been uncovered and not yet publicly disclosed.

50. Hope College's Notice Letter and Notice of Data Security Event have notably omitted any change to their data security or retention policies. These are steps that should have been employed in the first place-and which would have prevented or limited the impact of the Data Breach.

51. As a result of the Data Breach, Plaintiffs and Class Members have been and must continue to be vigilant and review their credit reports for incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

C. Hope College Failed to Comply with FTC Guidelines

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

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

54. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[4] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. *Id.*

55. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

[4] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016) (**Exhibit D** hereto).

suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

57. These FTC enforcement actions include actions against healthcare providers and partners like Hope College.

58. Hope College failed to properly implement basic data security practices.

59. Hope College's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

60. Hope College was at all times fully aware of the obligation to protect the PII of its students, applicants, employees, contractors, attendants of events at Hope College, and other persons who entrusted their PII to Hope College. Hope College was also aware of the significant repercussions that would result from its failure to do so.

61. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice that violates the FTC Act.

D. Hope College Failed to Comply with Data Security Industry Standards

62. Defendant is aware of the importance of safeguarding Plaintiffs' and Class Members' PII, that by virtue of their business—as a higher education institution—they place Plaintiffs' and Class Members' PII at risk of being targeted by cybercriminals.

63. Defendant is aware that the PII that they collect, organize, and store, can be used by cybercriminals to engage in crimes such as identity fraud and theft using Plaintiffs' and Class Members' PII.

64. Because Defendant failed to implement, maintain, and comply with necessary cybersecurity requirements, as a result, Defendant was unable to protect Plaintiffs' and Class Members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality.

65. As a proximate result of such failures, cybercriminals gained unauthorized access to Defendant's network and acquired Plaintiffs' and Class Members' PII in the Data Breach without being stopped.

66. Defendant was unable to prevent the Data Breach and was unable to detect the unauthorized access to vast quantities of sensitive and protected files containing Plaintiffs' and Class Members' PII.

67. Commonly accepted data security standards among businesses and higher education institutions that store personal information, such as the PII involved here, include, but are not limited to:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for personal and financial information;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

68. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for Cybersecurity (*Start with Security: A Guide for Business*, (June 2015)) and protection of personal and financial information (*Protecting Personal Information: A Guide for Business*, (Oct. 2016)), which includes basic security standards applicable to all types of businesses and higher education institutions.

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

70. Because Defendant was entrusted with Plaintiffs' and Class Members' PII, they had and have a duty to keep the PII secure.

71. Plaintiffs and Class Members reasonably expect that when they entrusted their PII to Hope College it will safeguard their information.

72. Despite Defendant's obligations, Defendant failed to appropriately monitor and maintain their data security systems in a meaningful way so as to prevent the Data Breach.

73. Had Defendant properly maintained their systems and adequately protected them, they could have prevented the Data Breach.

E. Defendant Violated Their Common Law Duty of Reasonable Care

74. Defendant was aware of the importance of security in maintaining personal information (particularly sensitive personal information like the PII involved here), and the value consumers place on keeping their PII secure.

75. In addition to obligations imposed by federal and state law, Defendant owed and continues to owe a common law duty to Plaintiffs and Class Members—who entrusted Defendant with their PII—to exercise reasonable care in receiving, maintaining, and storing, the PII in Defendant's possession.

76. Defendant owed and continues to owe a duty to prevent Plaintiffs' and Class Members' PII from being compromised, lost, stolen, accessed, or misused by unauthorized third parties. An essential part of Defendant's duty was (and is) the obligation to provide reasonable security consistent with current industry best practices and requirements, and to ensure information technology systems and networks, in addition to the personnel responsible for those systems and networks, adequately protected and continue to protect Plaintiffs' and Class Members' PII.

77. Defendant owed a duty to Plaintiffs and Class Members, who entrusted Defendant with extremely sensitive PII to design, maintain, and test the information technology systems that housed Plaintiffs' and Class Members' PII, to ensure that the PII in Defendant's possession was adequately secured and protected.

78. Defendant owed a duty to Plaintiffs and Class Members to create, implement, and maintain reasonable data security practices and procedures sufficient to protect the PII stored in Defendant's systems. In addition, this duty also required Hope College to adequately train its employees and others with access to Plaintiffs' and Class Members' PII on the procedures and practices necessary to safeguard such sensitive information. This duty also required supervision, training, and compliance on Hope College's part to ensure that it complied with creating, implementing, and maintaining reasonable data security practices and procedures sufficient to protect Plaintiffs' and Class Members' PII.

79. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would enable Defendant to timely detect a breach of its information technology systems, and a duty to act upon any data security warnings or red flags detected by such systems in a timely fashion.

80. Defendant owed a duty to Plaintiffs and Class Members to disclose when and if their information technology systems and data security practices were not sufficiently adequate to protect and safeguard Plaintiffs' and Class Members' PII.

81. As the Notice of Data Security Event states, "[u]pon discovery" of the "unauthorized access," Hope College immediately "began working with its IT team, and third-party forensic and legal specialists were engaged to conduct a full forensic investigation." Hope College could have—and should have—taken these steps *beforehand* to protect the PII in their possession and prevent the Data Breach from occurring, as required under the common law, FTC guidelines, as well as other state and federal law and/or regulations.

82. Thus, Defendant owed a duty to Plaintiffs and Class Members to timely disclose the fact that a data breach, resulting in unauthorized access to their PII, had occurred.

83. Defendant violated these duties. The Notice Letter and Notice of Data Security Event further states that Hope College became aware of the Data Breach on September 27, 2022, however Plaintiffs and Class Members, and the public did not learn of the Data Breach until December 15, 2022, when the Notice Letters were mailed out. Defendant failed to publicly describe the full extent of the Data Breach and notify affected parties. This demonstrates that Hope College did not properly implement measures designed to timely detect a data breach of their information technology systems, as required to adequately safeguard Plaintiffs' and Class Members' PII.

84. Defendant also violated their duty to create, implement, and maintain reasonable data security practices and procedures sufficient to protect Plaintiffs' and Class Members' PII.

85. Hope College breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Hope College's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- Failing to adequately protect customers' PII;
- Failing to properly monitor its own data security systems for existing intrusions;
- Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;
- Failing to detect unauthorized ingress into its systems;
- Failing to implement and monitor reasonable network segmentation to detect unauthorized travel within its systems, including to and from areas containing the most sensitive data;
- Failing to detect unauthorized exfiltration of the most sensitive data on its systems;
- Failing to train its employees in the proper handling of emails containing PII and maintain adequate email security practices;
- Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

- Failing to adhere to industry standards for cybersecurity as discussed above; and
- Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private PII.

86. Hope College negligently and unlawfully failed to safeguard Plaintiffs' and Class Members PII by allowing cybercriminals to access its computer network which contained unsecured and unencrypted PII.

87. Had Hope College remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Hope College could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

88. However, due to Hope College's failures, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Hope College.

F. Hope College Knew or Should Have Known that Criminals Target PII and the Data Breach was Foreseeable and Preventable

89. Defendant was well aware that the protected PII it acquires, stores, and utilizes is highly sensitive and of significant value to the owners of the PII and those who would use it for wrongful purposes.

90. PII is a valuable commodity to identity thieves, particularly when it is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal

information on anonymous websites, making the information widely available to a criminal underworld.

91. There is an active and robust market for this information. As John Sancenito, president of *Information Network Associates*, a company which helps companies with recovery after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers] do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."

92. PII is a valuable property right.[5] The value of PII as a commodity is measurable.[6] "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."[7] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[8] PII is so valuable to identity thieves that once PII has been

---

[5] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), 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 Feb. 24, 2023) (attached hereto as **Exhibit E**).

[6] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited Feb. 24, 2023) (attached hereto as **Exhibit F**).

[7] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited Feb. 24, 2023) (attached hereto as **Exhibit G**).

[8] *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 Feb. 24, 2023) (attached hereto as **Exhibit H**).

disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

93. 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, SSNs, PII, and 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.

94. The forms of PII involved in this Data Breach are particularly concerning and are a prime target for cybercriminals.

95. ***Social Security numbers***—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Social Security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

96. Indeed, even the Social Security Administration warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.

> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.

97. Social Security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often Social Security numbers can be used to obtain goods or services. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes Social Security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

98. ***Driver's license numbers***—are highly sought after by cyber criminals on the dark web because they are unique to a specific individual and extremely sensitive.

99. *Experian*, a globally recognized credit reporting agency, has explained "[n]ext to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves." This is because a driver's license number is connected to an individual's vehicle registration, insurance policies, records on file with the DMV and other government agencies, places of employment, doctor's offices, and other entities.

100. Further, unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, the type of PII at stake here—unique driver's license numbers—cannot be easily replaced.

101. For these reasons, driver's license numbers are highly sought out by cyber criminals because they are one of the most valuable pieces of information to facilitate identity theft and fraud. This information is valuable because cyber criminals can use this information to open credit card accounts, obtain insurance policies and submit fraudulent claims, open cell

phone contracts, file fraudulent tax returns, file unemployment applications, as well as obtain bank loans under a person's name.

102. The ramifications of Defendant's failure to keep Plaintiffs' and Class Members' PII secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their accounts *ad infinitum*.

103. Thus, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its systems were breached. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

104. As a highly sophisticated party that handles sensitive PII, Defendant failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and other Class Members' PII to protect against anticipated threats of intrusion of such information.

105. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a

new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

106. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

107. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[9]

108. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

109. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

110. The PII exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiffs and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

---

[9] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted), https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1310&context=jolt (last accessed Feb. 24, 2023) (attached hereto as **Exhibit I**).

111. There is often a lag time between when fraud occurs versus when it is discovered, as well as between when PII is stolen and when it is used. According to the *U.S. Government Accountability Office*, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

112. Personal information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black market for years. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[10] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[11]

113. Plaintiffs and Class Members rightfully place a high value not only on their PII, but also on the privacy of that data.

114. Thus, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they *will use it.*

115. Data breaches are preventable. As Lucy Thompson wrote in the *Data Breach and Encryption Handbook*, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security

---

[10] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last accessed Feb. 24, 2023) (attached hereto as **Exhibit J)**.

[11] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last accessed Feb. 24, 2023) (attached hereto as **Exhibit K**).

solutions." She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised…" and "[m]ost of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures…Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."

116. The types of PII, such as Social Security and driver's license numbers, compromised in the Data Breach are immutable. Plaintiffs and Class Members are not able to change them or simply cancel them, like a credit card, to avoid harm or fraudulent use of the information. Just like a birthdate or a mother's maiden name, these pieces of information cannot be changed by logging into a website and changing them in settings, and they can be used alone or in conjunction with other pieces of Plaintiffs' and Class Members' information to commit serious identity theft and fraud.

117. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[12] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. *Id.* at 4. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the

[12] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (emphasis added) (last accessed Feb. 24, 2023) (attached hereto as **Exhibit L**).

individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

118. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

119. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against entities like Hope College is to get information that they can monetize by selling it on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

120. It is within this context that Plaintiffs and all other Class Members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

121. Victims of the Data Breach, like Plaintiffs and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.

---

[13] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Feb. 24, 2023) (attached hereto as **Exhibit M**).

122. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class Members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, and credit reports for unauthorized activity for years to come.

G. Plaintiffs and Class Members Suffered Harm as a Result of the Data Breach

123. The ramifications of Defendant's failure to keep PII secure are long-lasting and severe. Victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time. In 2019 alone, consumers lost more than $1.9 billion to identity theft and fraud.

124. Besides damage sustained in the event of identity theft, consumers may also spend anywhere from approximately 7 hours to upwards to over 1,000 hours trying to resolve identity theft issues. The Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

125. Plaintiffs' PII was provided to Hope College in conjunction with the type of work Hope College performs as an educational institution. In requesting and maintaining Plaintiffs' PII, Hope College promised, and undertook a duty, to act reasonably in its handling of Plaintiffs' PII. Hope College, however, did not take proper care of Plaintiffs' PII, leading to its exposure to

and exfiltration by cybercriminals as a direct result of Hope College's inadequate data security measures.

126. On or around December 15, 2022, Hope College sent Plaintiffs notice concerning the Data Breach. The letter stated that Hope College experienced a data breach, and that the incident may have resulted in unauthorized access to Plaintiffs' personal information stored on Hope College's systems. According to Hope College, the compromised data included highly-sensitive information: first and last names, dates of birth, Social Security numbers, driver's license numbers, and student ID numbers. The notice further encouraged Plaintiffs "remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity." Hope College also offered free credit monitoring services through Cyberscout, but only for a period of 12 months.

127. As a result of Hope College's conduct and failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PII, which allowed the Data Breach to occur, Plaintiffs' PII has been and is now in the hands of unauthorized individuals and third parties, which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals.

128. Plaintiffs greatly value their privacy, especially their highly-sensitive information, such as their first and last names, dates of birth, Social Security numbers, and driver's license numbers. They would not have entrusted Hope College with this highly-sensitive information, had they known that Hope College would negligently fail to adequately protect their PII. Indeed, Plaintiffs provided Hope College with this highly-sensitive information with the expectation that Hope College would keep their PII secure and inaccessible from unauthorized parties.

129. As a result of Hope College's failure to implement and follow even the most basic security procedures, Plaintiffs 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 their personal information, and other economic and non-economic harm. Plaintiffs will now be forced to expend additional time to review their credit reports and monitor their financial accounts for fraud or identify theft—particularly since the compromised information may include Social Security numbers.

130. 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, Plaintiffs will need to maintain these heightened measures for years, and possibly their entire lives.

131. Plaintiffs are also at a continued risk of harm because their PII remains in Hope College's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Hope College fails to undertake the necessary and appropriate data security measures to protect the PII in its possession.

132. As a result of the Data Breach, and in addition to the time Plaintiffs have spent and anticipate spending to mitigate the impact of the Data Breach on their lives, Plaintiffs have also suffered emotional distress from the public release of their PII, which they believed would be protected from unauthorized access and disclosure. The emotional distress they have experienced includes anxiety and stress resulting from the fear that unauthorized bad actors are viewing, selling, and or using their PII for the purposes of identity theft and fraud.

133. Additionally, Plaintiffs have suffered damage to and diminution in the value of their highly sensitive and confidential PII—a form of property that Plaintiffs entrusted to Hope College and which was compromised as a result of the Data Breach Hope College failed to prevent. Plaintiffs have also suffered a violation of their privacy rights as a result of Hope College's unauthorized disclosure of their PII.

Plaintiff Jennie Devries

134. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Devries has spent approximately 1 to 2 hours monitoring her accounts for incidents of identity theft and fraud, or otherwise as a result of the Data Breach. The time spent monitoring her accounts as a result of the Data Breach is time Plaintiff Devries otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Devries lost was spent at Hope College's direction. Indeed, in the notice letter Plaintiff Devries received, Hope College directed Plaintiff Devries to spend time mitigating her losses by reviewing her accounts and credit reports for unauthorized activity.

135. Plaintiff Devries plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

136. Plaintiff Devries has also suffered emotional distress from the public release of her PII, which she did not even know that Hope College continued to possess and retain. The emotional distress she has experienced includes fear and anxiety, heartburn, loss of sleep, and ruminative thoughts resulting from unauthorized bad actors viewing, selling, and misusing her PII for the purposes of identity theft and fraud.

Plaintiff Timothy Drost

137. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Drost also experienced actual identity theft and fraud, including a drop in his credit score of 50 points. Plaintiff Drost has also experienced receipt of a substantial number of calls, emails, and text messages that do not appear to have any proper purpose.

138. Plaintiff Drost has spent approximately two hours responding to these incidents of identity theft and fraud, or otherwise as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Drost otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Drost lost was spent at Hope College's direction. Indeed, in the notice letter Plaintiff Drost received, Hope College directed Plaintiff Drost to spend time mitigating his losses by reviewing his accounts and credit reports for unauthorized activity.

139. Plaintiff Drost plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

140. Plaintiff Drost has also suffered emotional distress from the public release of his PII, which he believed would be protected from unauthorized access and disclosure. The emotional distress he has experienced includes anxiety and stress resulting from unauthorized bad actors viewing, selling, and misusing his PII for the purposes of identity theft and fraud.

Plaintiff Joseph Rodgers

141. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Rodgers has spent approximately 3 hours examining his accounts for incidents of identity theft and fraud, or otherwise as a result of the Data Breach. The time spent scouring his

records and being vigilant in response to the Data Breach is time Plaintiff Rodgers otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Rodgers lost was spent at Hope College's direction. Indeed, in the notice letter Plaintiff Rodgers received, Hope College directed Plaintiff Rodgers to spend time mitigating his losses by reviewing his accounts and credit reports for unauthorized activity.

142. Plaintiff Rodgers plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

143. Plaintiff Rodgers has also suffered emotional distress from the public release of his PII. The emotional distress he has experienced includes fear and anxiety, resulting from unauthorized bad actors viewing, selling, and misusing his PII for the purposes of identity theft and fraud.

Plaintiff Mark Cyphers

144. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Cyphers also experienced actual identity theft and fraud, including unauthorized charges to his debit/credit card(s), tax return(s) filed in his name, and credit issues. Plaintiff Cyphers has also experienced receipt of a substantial number of calls, emails, and text messages that do not appear to have any proper purpose.

145. Plaintiff Cyphers has spent approximately 60 to 70 hours responding to these incidents of identity theft and fraud, or otherwise as a result of the Data Breach. Plaintiff Cyphers spent time reviewing his financial accounts and statements, obtaining new debit/credit cards, freezing his credit, resetting automatic billing instructions tied to his business account, and

making efforts to secure credit monitoring services. Plaintiff Cyphers also incurred late/declined payment bank fees as a result of failed automatic payments.

146. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Cyphers otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Cyphers lost was spent at Hope College's direction. Indeed, in the notice letter Plaintiff Cyphers received, Hope College directed Plaintiff Cyphers to spend time mitigating his losses by reviewing his accounts and credit reports for unauthorized activity.

147. Plaintiff Cyphers plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

148. Plaintiff Cyphers has also suffered emotional distress from the public release of his PII. The emotional distress he has experienced includes fear and anxiety, resulting from unauthorized bad actors viewing, selling, and misusing his PII for the purposes of identity theft and fraud. The public release of his PII has also negatively impacted the operation of his business, which has caused Plaintiff Cyphers additional stress.

Plaintiff Emily Damaska

149. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Damaska also experienced actual identity theft and fraud, including a business checking account and business debit and credit cards being applied for in her name, a checking account being applied for and overdrawn in her name, a utilities account being opened in her name, loan applications being filed in her name, and a vehicle rental (where the vehicle was ultimately not returned) in her name. She has also experienced numerous hard inquiries on her credit, and received a substantial number of spam calls that do not appear to have any proper purpose.

150. Plaintiff Damaska has spent approximately 15 to 20 hours responding to these incidents of identity theft and fraud, or otherwise as a result of the Data Breach. For instance, Plaintiff Damaska has spent hours contacting banks, freezing her credit, placing a fraud alert on her credit, filing a police report, and monitoring her financial accounts. She has also downloaded a mobile application to block spam calls, and maintained credit monitoring and identity theft protection services since the Data Breach.

151. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Damaska otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Damaska lost was spent at Hope College's direction. Indeed, in the notice letter Plaintiff Damaska received, Hope College directed Plaintiff Damaska to spend time mitigating her losses by reviewing her accounts and credit reports for unauthorized activity.

152. Plaintiff Damaska plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

153. Plaintiff Damaska has also suffered emotional distress from the public release of her PII, which she believed would be protected from unauthorized access and disclosure. The emotional distress she has experienced includes fear, anxiety, and stress resulting from unauthorized bad actors viewing, selling, and misusing her PII for the purposes of identity theft and fraud. Plaintiff Damaska also plans on buying a house in the near future and is in the process of planning her wedding. The Data Breach has caused Plaintiff Damaska additional stress as she is worried about how the identity theft and fraud she has experienced will impact her ability to secure financing.

Plaintiff Elise Carter

154. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Carter also experienced actual identity theft and fraud, including a credit card and phone account being opened in her name. The phone account opened in her name was charged $799.00. Plaintiff Carter has also received a substantial number of calls, emails, and text messages that do not appear to have any proper purpose.

155. Plaintiff Carter has spent approximately 3 to 4 hours responding to these incidents of identity theft and fraud, or otherwise as a result of the Data Breach. For instance, Plaintiff Carter spent time making numerous phone calls to a credit card issuer and phone company to address the credit card and phone account opened in her name. She also spent time signing up for credit monitoring services. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Carter otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Carter lost was spent at Hope College's direction. Indeed, in the notice letter Plaintiff Carter received, Hope College directed Plaintiff Carter to spend time mitigating her losses by reviewing her accounts and credit reports for unauthorized activity.

156. Plaintiff Carter plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

157. Plaintiff Carter has also suffered emotional distress from the public release of her PII, which she believed would be protected from unauthorized access and disclosure. The emotional distress she has experienced includes fear and anxiety resulting from unauthorized bad actors viewing, selling, and misusing her PII for the purposes of identity theft and fraud.

Plaintiff Carter is also concerned that she may be required to deal with the Data Breach and public release of her PII for the rest of her life.

Plaintiff Tricia Garnett

158. Subsequent to the Data Breach, and in addition to the injuries alleged above, Plaintiff Garnett has spent approximately 4 hours investigating her accounts for potential incidents of identity theft and fraud, or otherwise as a result of the Data Breach. For instance, Plaintiff Garnett has spent time searching and reviewing her financial accounts on a monthly basis. The time spent dealing with these incidents resulting from the Data Breach is time Plaintiff Garnett otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff Garnett lost was spent at Hope College's direction. Indeed, in the notice letter Plaintiff Garnett received, Hope College directed Plaintiff Garnett to spend time mitigating her losses by reviewing her accounts and credit reports for unauthorized activity.

159. Plaintiff Garnett plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

160. Plaintiff Garnett has also suffered emotional distress from the public release of her PII, which she believed would be protected from unauthorized access and disclosure. The emotional distress she has experienced includes fear and anxiety resulting from unauthorized bad actors viewing, selling, and misusing her PII for the purposes of identity theft and fraud. She is also constantly worrying that her PII will be at risk for the rest of her life due to the public release of her Social Security number.

CLASS ACTION ALLEGATIONS

161. Plaintiffs brings this case individually and, pursuant to Rule 23(b)(2), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure, on behalf of the following Nationwide Class and state classes (collectively the "Class") (the Arizona, Indiana and Michigan Classes are collectively referred to as the "State Classes"):

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

In addition, or in the alternative, Plaintiffs propose the following state classes:

> **Arizona Class**
> All residents of Arizona whose PII was compromised in the Data Breach that was discovered by Hope College on or around September 27, 2022.
>
> **Indiana Class**
> All residents of Indiana whose PII was compromised in the Data Breach that was discovered by Hope College on or around September 27, 2022.
>
> **Michigan Class**
> All residents of Michigan whose PII was compromised in the Data Breach that was discovered by Hope College on or around September 27, 2022.
>
> (collectively, the "State Classes")

162. Excluded from the Class are Defendant, their subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

163. Plaintiffs reserve the right to modify or amend the definition of the proposed Class, if necessary, before this Court determines whether certification is appropriate.

164. The requirements of Rule 23(a)(1) are satisfied. The Class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. As noted above, there are approximately 156,783 Class Members.

165. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the information implicated in the Data Breach.

166. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting Class Members. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether and to what extent Defendant had a duty to secure and protect the PII of Plaintiffs and Class Members;

b. Whether Defendant were negligent in collecting and disclosing Plaintiffs' and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiffs' and Class Members' PII in the manner alleged herein, including failing to comply with industry standards;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant had respective duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

i. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

j. Whether Plaintiffs and Class Members are entitled to declaratory judgment under 28 U.S.C. § 2201, *et seq.*;

k. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

l. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

167. The requirements of Rule 23(a)(3) are satisfied. Plaintiffs' claims are typical of the claims of Class Members. The claims of the Plaintiffs and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard PII. Plaintiffs and Class Members each had their PII disclosed by Defendant to an unauthorized third party.

168. The requirements of Rule 23(a)(4) are satisfied. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class Members. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of Class Members and have no interests antagonistic to the Class Members. In addition, Plaintiffs has retained counsel who are competent and experienced in the prosecution of class action litigation, including data breach litigation. The claims of Plaintiffs and Class Members are substantially identical as explained above. While the aggregate damages that may be awarded to the Class Members are likely to be substantial, the damages suffered by the individual Class Members are relatively small. As a result, the expense and burden of individual litigation makes it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiffs and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class Member.

169. Here a class action is superior to other available methods for the fair and efficient adjudication of this controversy. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class Member are likely insufficient to

justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting damages in the aggregate would go un-remedied.

170. 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 Plaintiffs 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.

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 All Plaintiffs and the Nationwide Class or, Alternatively, the State Classes)

171. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

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

173. Hope College knew, or should have known, the risks of collecting and storing Plaintiffs' 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 Plaintiffs and Class Members.

174. 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.

175. Hope College breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class Members' PII.

176. It was reasonably foreseeable to Hope College that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class Members' PII to unauthorized individuals.

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

178. 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, Plaintiffs 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—a risk 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 identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of All Plaintiffs and the Nationwide Class, or Alternatively, the State Classes)

179. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

180. Hope College's duties arise from Section 5 of the FTCA ("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.

181. Hope College violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' 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 Plaintiffs and the other Class Members.

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

183. Plaintiffs and Class Members are within the class of persons that Section 5 of the FTCA was intended to protect.

184. 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.

185. It was reasonably foreseeable to Hope College that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class Members' PII to unauthorized individuals.

186. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Hope College's violations of Section 5 of the FTCA. Plaintiffs 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—a risk 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 identity theft they face and will continue to face; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of All Plaintiffs and the Nationwide Class or, Alternatively, the State Classes)

187. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

188. Plaintiffs 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. Plaintiffs 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 Plaintiffs' and Class Members' PII created a fiduciary relationship between Hope College and Plaintiffs and Class Members. In light of this relationship, Hope College must act primarily for the benefit of its students, applicants, employees, contractors, attendants of events at Hope College, and other persons who entrusted their PII to Hope College, which includes safeguarding and protecting Plaintiffs' and Class Members' PII.

189. Hope College has a fiduciary duty to act for the benefit of Plaintiffs 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 Plaintiffs' 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 Plaintiffs and Class Members it collected.

190. As a direct and proximate result of Hope College's breaches of its fiduciary duties, Plaintiffs 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 All Plaintiffs and the Nationwide Class or, Alternatively, the State Classes)

191. Plaintiffs reallege and incorporate 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).

192. Plaintiffs and Class Members conferred a monetary benefit upon Hope College in the form of monies paid for educational services or other services, or provision of employment or labor.

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

194. As a result of Hope College's conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their payments made or services provided with reasonable data privacy and security practices and procedures that

Plaintiffs and Class Members paid for, and those payments made or services provided without reasonable data privacy and security practices and procedures that they received.

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

196. Hope College should be compelled to provide for the benefit of Plaintiffs 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 All Plaintiffs and the Nationwide Class or, Alternatively, the State Classes)

197. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

198. Defendant required Plaintiffs 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 Plaintiffs and Class Members in which Hope College agreed to comply with its statutory and common law duties to protect Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

199. Plaintiffs 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.

200. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendant.

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

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

COUNT VI
MICHIGAN CONSUMER PROTECTION ACT
(Mich. Comp. Laws Ann §§ 445.901, *et. seq.*)
(On Behalf of Plaintiffs Devries, Cyphers, Drost, Damaska, and Carter and the Nationwide Class or, Alternatively, the Michigan Class)

203. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

204. 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.

205. Plaintiffs and Class Members provided PII to Defendant pursuant to transactions (i.e., providing education, goods, labor, employment, or services) they engaged in with Defendant, i.e., as customers, students, applicants, employees, contractors, and attendants of events at Hope College.

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

207. 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.

208. Hope College's deceptive trade practices include:

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

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' 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 Plaintiffs' and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45, and

f. Failing to timely and adequately notify Plaintiffs, and Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' 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 Plaintiffs and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45.

209. 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.

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

211. Hope College intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

212. Had Hope College disclosed to Plaintiffs 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 Plaintiffs, 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, Plaintiffs and the Class Members acted reasonably in relying on Hope College's misrepresentations and omissions, the truth of which they could not have discovered.

213. As a direct and proximate result of Hope College's deceptive trade practices, Plaintiffs 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.

214. Plaintiffs and Class Members are likely to be damaged by Hope College's ongoing deceptive trade practices.

215. Plaintiffs 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.

216. 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 Plaintiffs; (b) violation of Plaintiffs' 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.

COUNT VII
VIOLATION OF THE MICHIGAN IDENTITY THEFT PROTECTION ACT
Mich. Comp. Laws Ann. §§ 445.72, *et seq.*
(On Behalf of Plaintiffs Devries, Cyphers, Drost, Damaska, and Carter and the Nationwide Class or, Alternatively, the Michigan Class)

217. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

218. Defendant is a business that owns or licenses computerized data that includes PII as defined by Mich. Comp. Laws Ann. § 445.72(1).

219. Plaintiffs' and Class Members' personal information (for the purpose of this count, "PII"), (e.g., Social Security numbers) includes PII as covered under Mich. Comp. Laws Ann. § 445.72(1).

220. Defendant is required to accurately notify Plaintiffs and Class Members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

221. Because Defendant discovered a security breach and had notice of a security breach, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

222. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Mich. Comp. Laws Ann. § 445.72(4).

223. As a direct and proximate result of Defendant's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiffs and Class Members suffered damages, as described above.

224. Plaintiffs and Class Members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

COUNT VIII
INDIANA DECEPTIVE CONSUMER SALES ACT
Ind. Code §§ 24-5-0.5-1, *et seq.*
(On behalf of Plaintiff Rodgers and the Indiana Class)

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

226. Defendant is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

227. Defendant is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

228. Defendant engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

229. Defendant's representations and omissions include both implicit and explicit representations, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing

the risk of 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 Plaintiffs' and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

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

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45;

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

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45.

230. Defendant's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

231. The injury to consumers from Defendant's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk

to the safety of their PII or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

232. Consumers could not have reasonably avoided injury because Defendant's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Defendant created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

233. Defendant's inadequate data security had no countervailing benefit to consumers or to competition.

234. Defendant's acts and practices were "abusive" for numerous reasons, including:

a. Because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Defendant's failure to disclose the inadequacies in its data security interfered with consumers' decision-making in a variety of their transactions.

b. Because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Defendant's data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.

c. Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due

to the asymmetry in information between them and Defendant concerning the state of Defendant's security, and because it is functionally impossible for consumers to obtain credit without their PII being in Defendant's systems.

d. Because Defendant took unreasonable advantage of consumers' reasonable reliance that it was acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed below.

235. Defendant also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

a. Misrepresenting that the subject of a consumer transaction has performance, characteristics, or benefits it does not have which the supplier knows or should reasonably know it does not have;

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and

c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

236. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions.

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

238. Had Defendant disclosed to Plaintiff and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant 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. Defendant was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Class Members. Defendant accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

239. Defendant had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. This duty arose due to the representations and relationship between Defendant and Plaintiff Class Members as described herein. In addition, such a duty is implied by law due to the nature of the relationship between consumers-including Plaintiff Class Members and Defendant, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendant. Defendant's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff Class Members that contradicted these representations.

240. Defendant acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff and Class Members' rights. Defendant's actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

241. Defendant's conduct includes incurable deceptive acts that Defendant engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8). As a direct and proximate result of Defendant's uncured or incurable unfair, abusive, and deceptive acts or 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, as described herein, including but not limited to 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; loss of value of their PII; overpayment for Defendant's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

242. Defendant's violations present a continuing risk to Plaintiff and Class Members as well as to the public.

243. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

COUNT IX
ARIZONA CONSUMER FRAUD ACT
A.R.S. §§ 44-1521, *et seq*.
(On behalf of Plaintiff Garnett and the Arizona Class)

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

245. Defendant is a "person" as defined by A.R.S. § 44-1521(6).

246. Defendant advertised, offered, or sold goods or services in Arizona and engaged in trade or commerce directly or indirectly affecting the people of Arizona.

247. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A).

248. Defendant's unfair and deceptive acts and practices included:

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

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of 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 Garnett's and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

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

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Garnett's and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45;

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

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Garnett's and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45.

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

250. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions.

251. Had Defendant disclosed to Plaintiff Garnett and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant 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. Defendant was trusted with sensitive and valuable PII regarding thousands of consumers, including Plaintiff Garnett and Class Members. Defendant accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public.

Accordingly, Plaintiff Garnett and Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

252. Defendant acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiff Garnett's and Class Members' rights.

253. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff Garnett and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to 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; loss of value of their PII; overpayment for Defendant's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

Plaintiff Garnett and Class Members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT X
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of All Plaintiffs and the Nationwide Class or, Alternatively, the State Classes)

254. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

255. 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 grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

256. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and statutory duties to reasonably safeguard its

customers' sensitive personal information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches. Plaintiffs alleges that Defendant's data security practices remain inadequate.

257. Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their sensitive personal information and remain at imminent risk that further compromises of their personal information will occur in the future.

258. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant continues to owe a legal duty to secure consumers' sensitive personal information, to timely notify consumers of any data breach, and to establish and implement data security measures that are adequate to secure customers' sensitive personal information.

259. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect consumers' sensitive personal information.

260. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, for which they lack an adequate legal remedy. The threat of another data breach is real, immediate, and substantial. If another breach at Hope College occurs, Plaintiffs and Class Members will not have an adequate remedy at law, because not all of the resulting injuries are readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

261. The hardship to Plaintiffs and Class Members if an injunction does not issue greatly exceeds the hardship to Defendant if an injunction is issued. If another data breach occurs at Hope College, Plaintiffs and Class Members will likely be subjected to substantial identify theft and other damages. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

262. Issuance of the requested injunction will serve the public interest by preventing another data breach at Hope College, thus eliminating the additional injuries that would result to Plaintiffs and the thousands of consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for relief as follows:

(a) For an order certifying the National Class and Subclasses under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representative of the Class and/or Subclasses and Plaintiffs' attorneys as Class Counsel to represent the Class and Subclasses;

(b) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(c) For damages, including all compensatory, punitive, and/or nominal damages, in an amount to be determined by the trier of fact;

(d) For an order of restitution and all other forms of equitable monetary relief;

(e) Declaratory and injunctive relief as described herein;

(f) Awarding Plaintiffs reasonable attorneys' fees, costs, and expenses;

(g) Awarding pre- and post-judgment interest on any amounts awarded; and

(h) Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Dated: March 16, 2023

Respectfully submitted

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*
Samantha E. Holbrook*
134 Kings Hwy E., Fl. 2,
Haddonfield, NJ 08033
T: (856) 772-7200
F: (856) 210-9088
jshub@shublawyers.com
bjohns@shublawyers.com
sholbrook@shublawyers.com

LOWEY DANNENBERG, P.C.
Christian Levis*
Amanda G. Fiorilla*
44 South Broadway, Suite 1100
White Plains, NY 10601
T: (914) 997-0500
clevis@lowey.com
afiorilla@lowey.com

LOWEY DANNENBERG, P.C.
Anthony M. Christina*
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
T: (215) 399-4770
achristina@lowey.com

CHESTNUT CAMBRONNE PA
Bryan L. Bleichner
Philip J. Krzeski

100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
bbleichner@chesnutcambronne.com
pkrzeski@chestnutcambronne.com

THE LYON LAW FIRM, LLC
Joseph M. Lyon
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Charles R. Ash, IV (P73877)
ASH LAW, PLLC
402 W. Liberty St.
Ann Arbor, MI 48178
Phone: 734-234-5583
cash@nationalwagelaw.com

Terence R. Coates
Justin C. Walker
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com
dgould@msdlegal.com

Attorneys for Plaintiffs and the Proposed Class

**Pro Hac Vice Forthcoming*

CERTIFICATE OF SERVICE

I hereby certify that on March 16, 2023, I electronically filed the foregoing documents using the Court's electronic filing system, which will notify all counsel of record authorized to receive such filings.

/s/ E. Powell Miller
E. Powell Miller (P39487)
THE MILLER LAW FIRM, P.C.
950 W. University Dr., Ste. 300
Rochester, MI 48307
Tel: (248) 841-2200
epm@millerlawpc.com