UNITED STATED DISTRICT COURT
DISTRICT OF MINNESOTA

Conrad Segal and Madeline VanDerHeyden, *individually and on behalf of all others similarly situated,* Plaintiffs, v. University Of Minnesota, Defendant.	**Case No.** 0:23-cv-3114 **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Conrad Segal and Madeline VanDerHeyden ("Plaintiffs"), individually and on behalf of all others similarly situated, hereby bring this Class Action Complaint against University of Minnesota ("UMN" or "Defendant) and alleges, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and good faith belief as to all other matters, as follows:

NATURE OF THE ACTION

1. The University of Minnesota is the largest university in Minnesota and the second largest institution of higher education in the Midwest. Founded in 1851, it is a public research university and is comprised of five campuses Crookston, Duluth, Morris, Rochester, and the Twin Cities. The Twin Cities campus is the oldest and largest in the UMN system and has the ninth-largest main campus student body in the United States, with 52,376 students. According to

Defendant, the total cost of attending UMN for one academic year, two semester, is $35,632.00 for residents of Minnesota and $57,046.00 for out-of-state students.[1]

2. Students and prospective students, parents, employees and others provide UMN with highly sensitive personal information, including, among other things, names, birthdates, addresses, telephone numbers, email addresses, driver's license or passport information and social security numbers (collectively, "Private Information" or "PII") which UMN stores on its own university database.

3. UMN gathers, stores, and uses PII it gathers from students, applicants, employees, and other individuals. As such, UMN has a duty to protect the sensitive data it retains. Indeed, it admits to being governed by the Minnesota Government Data Practices Act ("MGDPA") and that it may not release personal information without the permission of the individual.[2] Further, under Minn. Stat. § 13.05, subd. 5(2) of the MGDPA, entities like UMN must "establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only accessed by those persons for purposes described in the procedure."

4. Despite the mandates of the MGDPA and UMN's understanding its need to implement reasonable security measures to keep PII safe, UMN failed to do so. Instead, a hacker active on the dark web with a username of "niggy" reported that he infiltrated UMN's database and gained access to PII and other sensitive information, including over 7 million unique social

[1] https://admissions.tc.UMN.edu/cost-aid/cost-aid-scholarships/cost-attendance (last accessed October 4, 2023).

[2] Online Privacy, UMN, https://privacy.umn.edu (last accessed Oct. 5, 2023).

security numbers ("Data Breach"). The stolen information includes data from digitized records initially created as far back as 1989.

5. Upon information and belief, UMN did not learn that the hacker had infiltrated and gained control over its systems to steal millions of social security numbers until after the hacker had successfully done so. Indeed, UMN only recently started investigating the Data Breach as of July 21, 2023. The hacker has already purported to have made the information available on the dark web.

6. Plaintiffs bring this class action against Defendant for its failure to properly secure and to safeguard the PII of Plaintiffs and Class Members from the unauthorized access of an unknown third party. Defendant's severe failures have affected—and continue to affect—over seven million people.

7. Although the PII of millions of victims was improperly exposed beginning in 2021, UMN did not begin notifying affected individuals of the Data Breach until some time in August 2023, approximately two years after the breach took place, thus depriving Plaintiffs and Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. In fact, UMN notified Plaintiffs that their PII was stolen by cybercriminals on September 28, 2023 – or more than two months after Defendant allegedly discovered the Data Breach. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiffs and Class Members has been driven even higher.

8. Upon information and good faith belief, Defendant was on notice of the high potential for this exact sort of data security incident and yet maintained the Private Information in a negligent manner. In particular, the Private Information was maintained on computer systems and networks that were in a condition vulnerable to cyberattack. Upon information and belief, the

mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant and, thus, Defendant were on notice that failing to take appropriate protective measures would expose and increase the risk that the Private Information could be compromised and stolen.

9. As a result, Plaintiffs' and Class Members' Private Information has been compromised and they now face an ongoing risk of identity theft, which is heightened here by the loss of Social Security numbers – the gold standard for identity thieves. The exposed Private Information of Plaintiffs and Class Members can, and likely will, be sold repeatedly on the dark web.

10. In addition to the ongoing risk of identity theft, those impacted by the Data Breach have suffered numerous actual and concrete injuries and damages, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of its Private Information; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

11. While many details of the Data Breach remain in the exclusive control of Defendant, upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain

reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiffs and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

12. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, future costs of identity theft monitoring, and injunctive relief including improvements to Defendant's data security systems, and future annual audits.

13. Plaintiffs therefore bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence; (ii) negligence *per se* (iii) breach of confidentiality; (iv) breach of fiduciary duty; (v) Violation of the Government Data Practices Act, Minn. Stat. § 13, *et seq.*; and (vi) breach of express contract.

PARTIES

14. Plaintiff Conrad Segal is a citizen of the State of Minnesota residing in Hennepin County, Minnesota. Plaintiff Segal was a student at UMN from 2012 to 2014. In his application, he provided UMN with his PII, including his name, contact information, Social Security Number, and date of birth, among other information.

15. Plaintiff Madeline VanDerHeyden is a citizen of the State of Minnesota residing in Hennepin County, Minnesota. Plaintiff VanDerHeyden did not attend UMN but was a prospective student UMN in 2011. In her application, she provided UMN with her PII, including her name, contact information, Social Security Number, and date of birth, among other information.

16. Plaintiffs received emails dated September 28, 2023 from Defendant notifying them that its network had been accessed and that their Private Information was involved in the Data Breach.

17. Defendant UMN is a higher education public institution in the State of Minnesota, organized under the laws of the State of Minnesota, with its principal place of business located at 100 Church Street SE, Minneapolis, MN.

JURISDICTION & VENUE

18. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiffs and at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million, exclusive of interest and costs. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business in this District and the computer systems implicated in

this Data Breach are likely based in this District. Further, Defendant is authorized to and regularly conducts business in this District and makes decisions regarding corporate governance and management of its businesses in this District, including decisions regarding the security measures to protect its clients' PII.

20. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because a substantial part of the events giving rise to this action occurred in this District, including decisions made by Defendant's governance and management personnel or inaction by those individuals that led to the Data Breach; Defendant's principal place of business is located in this district; Defendant maintains Class Members' PII in this District; and Defendant caused harm to Class Members residing in this District.

FACTUAL ALLEGATIONS

Defendant's Business

21. UMN is one of the nation's largest and most highly rated public higher education institutions in the nation. Tens of thousands of students and prospective students apply to attend UMN every year. UMN also employs tens of thousands of employees throughout its five campuses. As of 2022, UMN employed 4,033 academic staff, over 24,000 staff in general[3], and had nearly 55,000 students, including 30,560 undergraduates, 11,613 postgraduates, and 3,875 doctoral students.[4]

[3] https://idr.UMinn.edu/reports-by-topic-faculty-staff/faculty-and-staff-headcounts (last Accessed October 4, 2023).

[4] https://idr.UMinn.edu/reports-by-topic-enrollment/enrollments?utm_medium=browser&utm_id=oir_redirect&utm_source=0lYd6 (last Accessed October 4, 2023).

22. From its applicants, students, employees, and potential others, UMN collects highly sensitive PII, including names, addresses, telephone numbers, email addresses, birth dates, and social security numbers. Indeed, as part of its application process, UMN's online application portal requires U.S.-born applicants to provide their social security numbers.

23. As a condition of employment or admission, UMN requires applicants, students, employees and others to provide, and UMN collects and stores, highly sensitive personal information, including:

- Name;
- Address;
- phone number;
- email address;
- Date of birth;
- Demographic information and
- Social Security number.

24. UMN acknowledges that it is governed by the MGDPA in its Privacy Statement (the "Privacy Notice").[5] The current Privacy Notice has an effective date of November 2018. The Privacy Notice is posted on Defendant's website.

25. Defendant acquires, collects, and stores a massive amount of personally identifiable information from employees, prospective students, and students.

26. As a condition of employment or admission, Defendant requires that individuals entrust it with highly sensitive personal information. Indeed, as part of its application process,

[5] https://privacy.umn.edu/ (last accessed October 4, 2023).

UMN's online application portal requires U.S.-born applicants to provide their social security numbers.

27. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its employees, prospective students, and students, Defendant promises that the PII it collects and stores "is not released to external parties without your consent unless required by law."[6]

28. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

29. Defendant UMN understands the importance of securing the highly sensitive PII that it collects and stores in its database. In fact, UMN admits that, as a public institution, it is governed by the MGDPA.[7]

30. The MGDPA governs "all governmental entities" and was enacted to regulate the "collection, creation, storage, maintenance, dissemination, and access to government data in government entities." Under the MGDPA, government entities have obligations with respect to the data it collects and stores, including: (1) establish[ing] appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data and is only being accessed by those persons for purposes described in the procedure"; and "developing a policy incorporating these procedures, which may include a model policy governing

---

6 *Id.*

7 *Id.*

access to the data if sharing of the data with other government entities is authorized by law." *Id*. at § 13.05, subd. 5(a)(1)–(2).

31. The MGDPA, similarly, requires that "[w]hen not public data is being disposed of, the data must be destroyed in a way that prevents its contents from being determined." Id. at subd. 5(b). The MGDPA also required, starting more than two decades ago, that governmental entities "appoint or designate . . . [a] data practices compliance official" to resolve "problems in obtaining access to data or other data practices problems." *Id*. at subd. 13.

32. Furthermore, the MGDPA required UMN to obtain annual security assessments of any personal information maintained by the government entity. *Id*. at § 13.055, Subd. 6. Highlighting the significance of protecting data against unauthorized disclosure, when a breach does occur, the MGDPA requires government entities to notify impacted individuals "in the most expedient time possible and without unreasonable delay. . . ." *Id*. at subd. 2(a).

33. UMN acknowledges its obligations to protect data under the MGDPA, indicating that it is well aware of the importance of security data against unauthorized access.[8]

34. Despite its knowledge, UMN failed to enact measures sufficient to protect against a data breach and in August 2023, a hacker released millions of social security numbers and other PII stolen from a UMN database.

35. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

[8] *Id*.

36. Plaintiffs and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach

37. On August 22, 2023, the University of Minnesota confirmed that it had contacted law enforcement concerning a potential data breach of which it had become aware on July 21, 2023.[9] Specifically, representatives of UMN stated that they became aware that an "unauthorized party" had claimed to possess sensitive data taken from UMN's computer systems.[10]

38. UMN became aware of the data breach from disclosures made by the purported hacker. On July 21, 2023, a hacker with a username "niggy" posted on the dark web and claimed to have accessed UMN's database and obtained sensitive information, including social security numbers, for over seven million unique individuals.[11] The hacker exploited a Computer Network Exploitation or "CNE," which is often used to infiltrate a target's computer networks to extract and gather data. The hacker here successfully breached UMN's database, uncovering sensitive information dating back to records initially created in 1989 and later digitized.[12]

---

9 https://www.kare11.com/article/news/local/u-of-m-investigating-claimeddatabreach/89-17a1736f-a704-4495-9337-079e0c77ccd5 (last accessed Oct. 5, 2023).

10 *Id*.

11 https://thecyberexpress.com/university-of-minnesota-data-breach/ ((last accessed Oct. 5, 2023).

12 *Id*.

39. The Data Breach affected individuals who submitted information to Defendant as prospective students, attended UMN as a student, worked at UMN as an employee, or participated in UMN programs between 1989 and August 2021.

40. Former UMN regent Michael Hsu warned that "everyone should be concerned" because "even if you are a former student or staff you still have data in the university system."[13]

41. Mark Lanterman, the Chief Technology Officer at Computer Forensic Services, warned that anyone potentially affected by the Data Breach should freeze their credit reports to prevent new credit being opened in their names.[14]

42. According to UMN, they have run scans which indicate no ongoing suspicious activity.[15] Thus, the hacker successfully entered into UMN's networks, gained access to UMN's database, exfiltrated a significant quantity of data, including PII, all without detection by UMN or any of its security tools or personnel. Indeed, UMN only became aware of the attack after the hacker publicly described it and posted the stolen data.

43. Defendant's Notice of Data Breach admits that Plaintiffs' and Class Members' Private Information was accessed without authorization.

Plaintiff Conrad Segal's Experience

44. As a requisite to attending graduate school at the University of Minnesota, Plaintiff Segal provided his Private Information to Defendant in 2012 and trusted that the information would be safeguarded according to state and federal law. Upon receipt, Plaintiff Segal's PII was entered and stored in Defendant's network and systems.

---

13 *Supra*, n. 10.

14 *Id*

.

15 *Id.*

45. Plaintiff Segal is very careful about sharing his sensitive Private Information, and he has never knowingly transmitted unencrypted sensitive Private Information.

46. Plaintiff Segal stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Segal diligently chooses unique usernames and passwords for his various online accounts. Had he known Defendant failed to follow basic industry security standards and failed to implement systems to protect his Private Information, he would not have provided that information to Defendant.

47. Defendant's Notice Letter, dated September 28, 2023, notified Plaintiff Segal that its network had been accessed and Plaintiff Segal's Private Information may have been involved in the Data Breach, which included Plaintiff Segal's name, date of birth, address, and social security number.

48. Furthermore, Defendant directed Plaintiff Segal to be vigilant and to take certain steps to protect his Private Information and otherwise mitigate her damages.

49. As a result of the Data Breach, Plaintiff Segal heeded Defendant's warning and spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff Segal to mitigate his damages by, among other things, monitoring his online accounts and credit reports for unauthorized activities.

50. However, even with the most diligent response, the harm caused to Plaintiff Segal cannot be undone.

51. Plaintiff Segal further suffered actual injury in the form of damages to and diminution in the value of Plaintiff Segal's Private Information—a form of intangible property that Plaintiff Segal entrusted to Defendant, which was compromised as a result of the Data Breach.

52. Plaintiff Segal also lost his benefit of the bargain by paying for educational services that failed to provide the data security that was promised.

53. Plaintiff Segal suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

54. Plaintiff Segal has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals.

55. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

56. Plaintiff Segal has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Madeline VanDerHeyden's Experience

57. As a requisite to applying for acceptance at the University of Minnesota, Plaintiff VanDerHeyden provided her Private Information to Defendant in 2011 and trusted that the information would be safeguarded according to state and federal law. Upon receipt, Plaintiff VanDerHeyden's PII was entered and stored in Defendant's network and systems.

58. Plaintiff VanDerHeyden is very careful about sharing her sensitive Private Information, and she has never knowingly transmitted unencrypted sensitive Private Information.

59. Plaintiff VanDerHeyden stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff VanDerHeyden diligently chooses unique usernames and passwords for her various online accounts. Had she known Defendant failed to follow basic industry security standards and failed to implement systems to protect her Private Information, she would not have provided that information to Defendant.

60. Defendant's Notice Letter, dated September 28, 2023, notified Plaintiff VanDerHeyden that its network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach, which included Plaintiff VanDerHeyden's name, date of birth, address, and social security number.

61. Furthermore, Defendant directed Plaintiff VanDerHeyden to be vigilant and to take certain steps to protect her Private Information and otherwise mitigate her damages.

62. As a result of the Data Breach, Plaintiff VanDerHeyden heeded Defendant's warning and spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff VanDerHeyden to mitigate her damages by, among other things, monitoring her online accounts and credit reports for unauthorized activities.

63. However, even with the most diligent response, the harm caused to Plaintiff VanDerHeyden cannot be undone.

64. Plaintiff VanDerHeyden further suffered actual injury in the form of damages to and diminution in the value of Plaintiff VanDerHeyden's Private Information—a form of

intangible property that Plaintiff VanDerHeyden entrusted to Defendant, which was compromised as a result of the Data Breach.

65. She also lost his benefit of the bargain by paying for educational services that failed to provide the data security that was promised.

66. Plaintiff VanDerHeyden suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

67. Plaintiff VanDerHeyden has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and possibly criminals.

68. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

69. Plaintiff VanDerHeyden has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

The Data Breach Was Eminently Foreseeable

70. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

71. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially millions of

individuals' detailed, personal information and thus the significant number of individuals who would be harmed by the exposure of the unencrypted data.

72. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[16]

73. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the education sector preceding the date of the breach.

74. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[17] The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

75. Compared to 2021, the education sector experienced a 44% increase in cyber-attacks in 2022, with an average of 2297 attacks against organizations every week.[18]

76. In light of recent high profile cybersecurity incidents at other educational institutions, Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

---

[16] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed October 4, 2023).

[17] *See* 2021 Data Breach Annual Report, 6 (ITRC, Jan. 2022) available at https://notified.idtheftcenter.org/s/ (last accessed October 4, 2023).

[18] https://www.infosecurity-magazine.com/news/education-experienced-44-increase/ (last accessed Oct. 5, 2023).

77. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities "are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to its data quickly."[19]

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

Value of PII

79. The PII of consumers remains of high value to criminals, as evidenced by the prices offered through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[20] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[21]

80. For instance, cybercriminals on the dark web have sold Social Security numbers for up to $300 per number to be used on fraudulent tax returns. UMN's data breach exposed social security numbers, which are already available on the dark web.

---

[19] FBI, Secret Service Warn of Targeted Ransomware, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/ (last accessed Oct. 5, 2023).

[20] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Oct. 5, 2023).

[21] *In the Dark*, VPNOverview, 2019, available at https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Oct. 5, 2023).

81. After a data breach like the one at UMN, the hackers responsible for the breach increasingly seek to sell the stolen personal and sensitive records on the black market to purchasers looking to use the PII to create fake IDs, make fraudulent transactions, obtain loans, or commit other acts of identity theft.[22]

82. Given the value of that data, a robust cyber black market exists in which criminals openly post and purchase stolen personal information on the dark web.

83. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

84. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information…[is] worth more than 10x on the black market."[23]

85. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing, or even give false information to police.

86. Additionally, after personal information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can allow hackers to harvest additional sensitive and confidential information

---

[22] *How do hackers make money from your stolen data?*, Emsisoft.com (Feb. 20, 2020), https://blog.emsisoft.com/en/35541/how-do-hackers-make-money-from-your-stolen-data (last accessed Oct. 5, 2023).

[23] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers,* IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Oct. 5, 2023).

from the victim, as well as the personal information of family, friends, and colleagues of the initial victim.

87. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individual and business victims. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant here did not timely report to Plaintiff and the Class that their personal information had been stolen and, in fact, have not reported the full extent of the Data Breach to date.

88. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts. Using data stolen in data breaches like UMN's, hackers and other wrongdoers may use consumers' personal and financial information to siphon money from existing accounts, open new accounts in the names of their victims, or sell consumers' personal information to others who do the same.

89. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit.

90. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of identity theft, not to mention the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their personal information. Victims of new account identity theft will likely have to spend time correcting fraudulent

information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

91. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen personal information. To protect themselves, Plaintiffs and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

92. According to the U.S. Government Accountability Office ("GAO"), 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.[24]

93. As a result, victims suffer immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

94. Even absent any adverse use, consumers suffer injury from the simple fact that their PII has been stolen. When personal information, especially social security numbers, is stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. In short, this information can no longer guarantee Plaintiffs' and Class Members' identities.

95. As such, future monitoring of financial and personal records is reasonable and necessary well beyond the one year of protection offered by Defendant.

Defendant Failed to Properly Protect Plaintiffs' and Class Members' Private Information

[24] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at*: https://www.gao.gov/assets/gao-07-737.pdf (last accessed Oct. 5, 2023).

96. Defendant UMN could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom its relationship had ended a significant period of time prior to the breach – including Plaintiff Segal who last attended UMN in 2014 and Plaintiff VanDerHeyden who never attended UMN and whose application to attend was submitted in 2011.

97. Defendant UMN's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

98. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

99. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[25]

[25] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, Fed. Trade Comm., https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last accessed Oct. 5, 2023).

100. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

101. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[26]

102. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks…

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)…

[26] *Id.* at 3-4.

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic…[27]

103. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

[27] *See* Cybersecurity & Infrastructure Security Agency, *Protecting Against Ransomware* (original release date Apr. 11, 2019), https://www.cisa.gov/news-events/news/protecting-against-ransomware (last accessed Oct. 5, 2023).

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[28]

104. Moreover, given that Defendant was storing the PII of Plaintiffs and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

105. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of Plaintiffs and Class Members.

106. As a result of computer systems in need of security upgrades and inadequate procedures for handling email phishing attacks, viruses, malignant computer code, and hacking

[28] *See Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed Oct. 5, 2023).

attacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

107. Because Defendant failed to properly protect and safeguard Plaintiffs' and Class Members' Private Information, an unauthorized third party was able to access Defendant's network, and access Defendant's database and system configuration files and exfiltrate that data.

Defendant Failed to Comply with FTC Guidelines

108. The Federal Trade Commission ("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.

109. 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 patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[29]

110. 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.

[29] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016),https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Oct. 5, 2023).

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

112. The FTC has brought enforcement actions against businesses for failing to protect patient data adequately and reasonably, 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 clarify the measures businesses take to meet its data security obligations.

113. Defendant failed to properly implement basic data security practices.

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

115. Defendant was always fully aware of its obligation to protect the Private Information of Plaintiffs and Class Members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant's Negligent Acts & Breaches

116. Defendant participated and controlled the process of gathering the Private Information from Plaintiffs and Class Members.

117. Defendant therefore assumed and otherwise owed duties and obligations to Plaintiffs and Class Members to take reasonable measures to protect the information, including the

duty of oversight, training, instruction, testing of the data security policies and network systems. Defendant breached these obligations to Plaintiffs and Class Members and/or were otherwise negligent because it failed to properly implement data security systems and policies for its network that would adequately safeguarded Plaintiffs' and Class Members' Sensitive Information.

118. Upon information and belief, Defendant's unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

a) Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiffs' and Class Members Private Information;

b) Failing to properly monitor its data security systems for data security vulnerabilities and risk;

c) Failing to test and assess the adequacy of its data security system;

d) Failing to develop adequate training programs related to the proper handling of emails and email security practices;

e) Failing to put into develop and place uniform procedures and data security protections for its healthcare network;

f) Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g) Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;

h) Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;

i) Failing to implement or update antivirus and malware protection software in need of security updating;

j) Failing to require encryption or adequate encryption on its data systems;

k) Otherwise negligently and unlawfully failing to safeguard Plaintiffs' and Class Members' Private Information provided to Defendant, which in turn allowed cyberthieves to access its IT systems.

COMMON INJURIES & DAMAGES

119. As result of Defendant's ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

120. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of its Private Information; and (i) the continued risk to its Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

The Risk of Identity Theft to Plaintiffs & Class Members Is Present and Ongoing

121. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

122. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

123. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

124. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[30] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[31] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

---

30 *What Is the Dark Web?,* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last accessed Oct. 5, 2023).

31 *Id.*

125. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.[32]

126. The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain its anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[33] As Microsoft warns, "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[34]

127. Social Security numbers, for example, are among the worst kinds of personal information to have been stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you

---

32 *What is the Dark Web*? https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last accessed Oct. 5, 2023).

33 *Id*.

34 *Id*.

> never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[35]
>
> What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

128. Even then, 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."[36]

129. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

130. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[37]

---

[35] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Oct. 5, 2023).

[36] 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 Oct. 5, 2023).

[37] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Oct. 5, 2023).

131. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached its highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[38]

132. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[39] Defendant did not rapidly report to Plaintiffs and the Class that its Private Information had been stolen.

133. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

134. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in its credit reports and continuously monitor its reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

135. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

---

38 *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last accessed Oct. 5, 2023).

39 *Id.*

136. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why its information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[40]

137. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.

138. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[41]

139. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to

---

[40] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last accessed Oct. 5, 2023).

[41] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Oct. 5, 2023).

protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[42]

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

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

141. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that its Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

142. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendant's Notice instructs them, "monitor your online accounts and credit reports for unauthorized activities" and "report any suspicious activities to appropriate law enforcement."

143. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing

[42] *See, e.g.*, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices (last accessed Oct. 5, 2023).

passwords, reviewing and monitoring credit reports and accounts for unauthorized activity—which may take years to discover and detect—and filing police reports.

144. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office, who released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to its good name and credit record."[43]

145. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect its personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals its identity), reviewing its credit reports, contacting companies to remove fraudulent charges from its accounts, placing a credit freeze on its credit, and correcting its credit reports.[44]

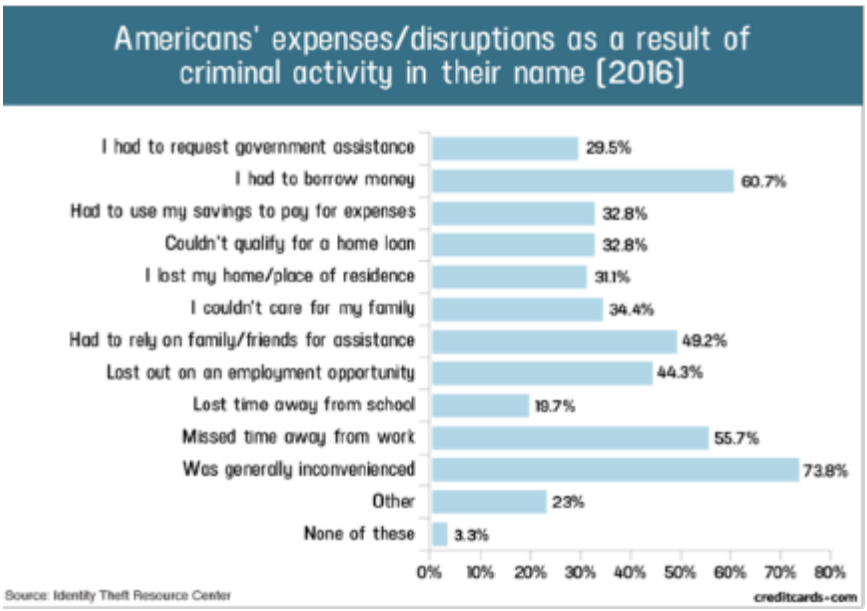
146. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[45]

---

[43] *See* United States Government Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed Oct. 5, 2023).

[44] *See* Federal Trade Commission, IdentityTheft.com, https://www.identitytheft.gov/Steps (last accessed Oct. 5, 2023).

[45] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



147. In the event that Plaintiffs and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to its good name and credit record."[46] Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect its personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals its identity), reviewing its credit reports, contacting companies to remove fraudulent charges from its accounts, placing a credit freeze on its credit, and correcting its credit reports.[47]

---

[46] *See Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed Oct. 5, 2023). ("GAO Report").

[47] *See* https://www.identitytheft.gov/Steps.

Injunctive Relief Is Necessary to Protect Against Future Data Breaches

148. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

CLASS ACTION ALLEGATIONS

149. Plaintiffs bring this action on behalf of themselves and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seek certification of the following Nationwide Class:

> All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach.

150. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

151. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

152. **Numerosity**. Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiffs believe that there are millions of members of the Nationwide Class. The number of

reportedly impacted individuals already exceeds 7 million U.S. individuals—and each persons' information is readily available to download on the dark web. The precise number of class members, however, is not yet known to Plaintiffs. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

153. **Commonality and Predominance**. Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any questions affecting individual Class members. These common questions include, without limitation:

a. Whether UMN knew or should have known that its data environment and cybersecurity measures created a risk of a data breach;

b. Whether UMN controlled and took responsibility for protecting Plaintiffs' and the Class's data when it solicited that data, collected it, and stored it on its servers;

c. Whether UMN's security measures were reasonable in light of the FTC data security recommendations, state laws and guidelines, industry standards, and common recommendations made by data security experts;

d. Whether UMN breached the MGDPA by implementing and using unreasonable data security measures;

e. Whether UMN owed Plaintiffs and the Class a duty to implement reasonable security measures;

f. Whether UMN's failure to adequately secure Plaintiffs' and the Class's data constitutes a breach of its duty to institute reasonable security measures;

g. Whether UMN's failure to implement reasonable data security measures allowed the breach of its data systems to occur and caused the theft of Plaintiffs' and the Class's data;

h. Whether reasonable security measures known and recommended by the data security community could have prevented the breach;

i. Whether Plaintiffs and the Class were injured and suffered damages or other losses because of UMN's failure to reasonably protect its data systems; and

j. Whether Plaintiffs and the Class are entitled to relief.

154. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs are typical members of the Class. Plaintiffs and the Class are each persons who provided data to UMN, whose data resided on UMN's servers, and whose personally identifying information was exposed in the Data Breach. Plaintiffs' injuries are similar to other class members and Plaintiffs seek relief consistent with the relief due to the Class.

155. **Adequacy**. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against UMN to obtain relief for themselves and for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs also have retained counsel competent and experienced in complex class action litigation of this type, having previously litigated numerous data breach cases on behalf of consumers and financial institutions. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

156. **Superiority**. Consistent with Fed. R. Civ. P 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy. Individual litigation by each Class member would strain the court system because of the numerous members of the Class. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides

the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit customers to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

157. **Injunctive and Declaratory Relief**. Consistent with Fed. R. Civ. P. 23(b)(2), UMN, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

CAUSES OF ACTION

COUNT I

Negligence
(*On Behalf of Plaintiffs & All Class Members*)

158. Plaintiffs and the Class repeat and re-allege all other paragraphs of the Complaint as if fully set forth herein.

159. Upon gaining access to the PII of Plaintiffs and members of the Class, Defendant owed to Plaintiffs and the Class a duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed, and misused by unauthorized parties. Pursuant to this duty, Defendant was required to design, maintain, and test its security systems to ensure that these systems were reasonably secure and capable of protecting the PII of Plaintiffs and the Class. Defendant further owed to Plaintiffs and the Class a duty to implement systems and procedures that would detect a breach of its security systems in a timely manner and to timely act upon security alerts from such systems.

160. Defendant owed this duty to Plaintiffs and the other Class Members because Plaintiffs and the other Class Members compose a well-defined, foreseeable, and probable class

of individuals whom Defendant should have been aware could be injured by Defendant's inadequate security protocols. Defendant actively solicited students and employees who entrusted Defendant with Plaintiffs' and the other Class Members' PII. To facilitate these services, Defendant used, handled, gathered, and stored the PII of Plaintiffs and the other Class Members. Attendant to Defendant's solicitation, use and storage, Defendant knew of its inadequate and unreasonable security practices with regard to its computer/server systems and also knew that hackers and thieves routinely attempt to access, steal and misuse the PII that Defendant actively solicited from clients who entrusted Defendant with Plaintiffs' and the other Class Members' data. As such, Defendant knew a breach of its systems would cause damage to its clients and Plaintiffs and the other Class Members. Thus, Defendant had a duty to act reasonably in protecting the PII of its healthcare clients' patients.

161. The duty included obligations to take reasonable steps to prevent disclosure of the Private Information, and to safeguard the information from theft. Defendant's duties included the responsibility to design, implement, and monitor data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

162. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the Private Information.

163. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its employees, students, and prospective students, which is recognized by laws and regulations including but not limited to the

FTC Act, and common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

164. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

165. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information that it either acquires, maintains, or stores.

166. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information, as alleged and discussed above.

167. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

168. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

169. The imposition of a duty of care on Defendant to safeguard the Private Information it maintained is appropriate because any social utility of Defendant's conduct is outweighed by the injuries suffered by Plaintiffs and Class Members as a result of the Data Breach.

170. Defendant was also negligent in failing to timely notify Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

171. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to its Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

172. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

173. Defendant's negligent conduct is ongoing, in that it still hold the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

174. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II

Negligence *Per Se*
(*On Behalf of Plaintiffs & All Class Members*)

175. Plaintiffs and the Class repeat and re-allege all other paragraphs of the Complaint as if fully set forth herein.

176. Pursuant to Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

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

178. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

179. Additionally, the MGDPA requires entities like UMN to "establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data and is only being accessed by those persons for purposes described in the procedure[.]" Minn. Stat. § 13.05, subd. 5(a)(1). Additionally, the MGDPA requires entities to notify those impacted by a data "in the most expedient time possible and without unreasonable delay . . . ." *Id.* at Subd. 2(a).

180. Defendant UMN violated Section 5 of the FTC Act and the MGDPA by failing to use reasonable measures to protect Plaintiffs' and the Class's PII and sensitive data and by not complying with applicable industry standards. UMN's conduct was particularly unreasonable

given the sensitive nature and amount of data it stored on its databases and the foreseeable consequences of a Data Breach should UMN fail to secure its systems.

181. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act and the MGDPA, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

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

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

184. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of its Private Information.

185. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III

Breach of Confidence
(*On Behalf of Plaintiffs & All Class Members*)

186. Plaintiffs and the Class repeat and re-allege all other paragraphs of the Complaint as if fully set forth herein.

187. At all times during its possession and control of Plaintiffs' and Class Members' Private Information, Defendant was fully aware of the confidential, novel, and sensitive nature of Plaintiffs' and Class Members' Private Information provided to it.

188. As alleged herein and above, Defendant's possession and control of Plaintiffs' and Class Members' highly sensitive Private Information was governed by the expectations of Plaintiffs and Class Members that its Private Information would be collected, stored, and protected in confidence, and that it would not be disclosed to unauthorized third parties.

189. Plaintiffs and Class Members provided their respective Private Information with the understanding that it would be protected and not disseminated to any unauthorized parties.

190. Plaintiffs and Class Members also provided its respective Private Information with the understanding that precautions would be taken to protect it from unauthorized disclosure, and that these precautions would at least include basic principles of information security practices.

191. Defendant voluntarily received, in confidence, Plaintiffs' and Class Members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

192. Due to Defendant's failure to prevent, detect, and/or avoid the Data Breach from occurring by, inter alia, failing to follow best information security practices to secure Plaintiffs' and Class Members' Private Information, Plaintiffs' and Class Members' Private Information was

disclosed and misappropriated to unauthorized criminal third parties beyond Plaintiffs' and Class Members' confidence, and without its express permission.

193. But for Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Private Information, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third-party criminals. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' Private Information, as well as the resulting damages.

194. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Private Information. Defendant knew or should have known that its security systems were insufficient to protect the Private Information that is coveted and misused by thieves worldwide. Defendant also failed to observe industry standard information security practices.

195. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members suffered damages as alleged herein.

COUNT IV

Breach of Fiduciary Duty
(*On Behalf of Plaintiffs & All Class Members*)

196. Plaintiffs and the Class repeat and re-allege all other paragraphs of the Complaint as if fully set forth herein.

197. In providing their Private Information to Defendant, Plaintiffs and Class Members justifiably placed a special confidence in Defendant to act in good faith and with due regard for the interests of Plaintiffs and Class Members to safeguard and keep confidential that Private Information.

198. Defendant accepted the special confidence Plaintiffs and Class Members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiffs' personal information as included in the Data Breach notification letter.

199. In light of the special relationship between Defendant, Plaintiffs, and Class Members, whereby Defendant became a guardian of Plaintiffs and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiffs and Class Members for the safeguarding of Plaintiffs and Class Members' Private Information.

200. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationships, in particular, to keep secure the Private Information of its students, applicants, and employees and to timely notify Plaintiffs and Class Members of a data breach and disclosure.

201. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

202. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs and Class Members' Private Information.

203. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

204. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to:

a. Actual identity theft;

b. The compromise, publication, and/or theft of its Private Information;

c. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of its Private Information;

d. Lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft;

e. The continued risk to its Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession and

f. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

205. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members will suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V

Violation of Government Data Practices Act, Minn. Stat. § 13, *et seq*.
(*On Behalf of Plaintiffs & All Class Members*)

206. Plaintiffs and the Class repeat and re-allege all other paragraphs of the Complaint as if fully set forth herein.

207. Under the MGDPA, a government entity that "violates any provision of this chapter is liable to a person or representative of a decedent who suffers any damages as a result of the violation, and the person damaged . . . may bring an action against the responsible authority or government entity to cover any damages sustained, plus costs and reasonable attorney's fees." Minn. Stat. § 13.08, subd. 1.

208. Furthermore, "[t]he state is deemed to have waived any immunity to a cause of action brought under this chapter." *Id.* Additionally, the MGDPA states that "[a] responsible authority or government entity which violates or purposes to violate this chapter may be enjoined by the district court." *Id.* at subd. 2.

209. The MGDPA governs the UMN and applies to its storage of Plaintiffs' and the Class's personal information. Minn. Stat. § 13.01, subd. 1 ("All governmental entities shall be governed by this chapter.").

210. Under the MGDPA, the UMN was required to "establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure." Minn. Stat. § 13.05, subd. 5(a)(2).

211. Furthermore, the MGDPA required UMN to obtain annual security assessments of any personal information maintained by the government entity. *Id.* at § 13.055, subd. 6. Highlighting the significance of protecting data against unauthorized disclosure, when a breach does occur, the MGDPA requires government entities to notify impacted individuals "in the most expedient time possible and without unreasonable delay . . . ." *Id.* at subd. 2(a).

212. UMN acknowledges its obligations to protect data under the MGDPA, indicating that it is well aware of the importance of security data against unauthorized access.[48]

213. However, UMN failed to adopt "appropriate security safeguards" to protect Plaintiffs' and the Class's highly sensitive information that it stored in its database. The lack of appropriate security safeguards is made clear by the means by which the Data Breach occurred.

[48] https://privacy.umn.edu/

Specifically, a single hacker with no apparent history of orchestrating data breaches as part of a cybercrime organization singlehandedly infiltrated UMN, obtained control over its networks and access to its databases, successfully exfiltrated a massive amount of data involving over 7 million individuals, and exfiltrated that data all without detection. UMN had no idea it had been breached and the data on its databases stolen until the hacker publicly disclosed the breach and, by the time UMN began investigating it, the hacker, having succeeded in obtaining a swath of valuable data, had already ceased activity within UMN's networks and servers.

214. UMN, therefore, violated the MGDPA.

215. Plaintiffs, furthermore, suffered damage as a result of the Data Breach, which occurred directly because of UMN's violation of the MGDPA and its failure to adopt appropriate security safeguards.

216. Specifically, Plaintiffs' and the Class's highly sensitive information has been placed on the dark web where cybercriminals have access to it and opportunity to misuse it. Consequently, the confidentiality, integrity, and value of this sensitive information has been diminished because it can no longer guarantee Plaintiffs' and the Class's identities. Plaintiffs and the Class were also damaged due to the need to expend time, effort, and money monitoring their financial accounts, social media applications and their credit scores to identify any misuse of their data. Plaintiffs, in fact, remained at a heightened and substantial risk of harm due to the misuse of their data which has been placed directly in the hands of criminals. Finally, Plaintiffs suffered emotional distress stemming from the disclosure of their sensitive data and the heightened and prolonged risk of harm they now suffer.

217. Plaintiffs, therefore, seek to recover the damages they suffered and costs and attorneys' fees.

COUNT VI

Breach of Contract
(*On Behalf of Plaintiffs & All Class Members*)

218. Plaintiffs and the Class repeat and re-allege all other paragraphs of the Complaint as if fully set forth herein.

219. Plaintiffs and Members of the Class allege that they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts, with Defendant for the provision of employment and educational services.

220. Specifically, Plaintiffs entered into a valid and enforceable express contract with Defendant when Plaintiffs first applied, enrolled or were employed by Defendant.

221. The valid and enforceable express contracts to provide employment and educational services that Plaintiffs and Class Members entered with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant gather on its own from disclosure.

222. Under these express contracts, Defendant promised and was obligated to: (a) provide educational services and employment to Plaintiffs and Class Members; and (b) protect Plaintiffs and the Class Members' PII: (i) provided to obtain such educational services and employment; and/or (ii) created as a result of providing such educational services and employment. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services or provide their labor, and to turn over their Private Information.

223. Both the provision of educational services and employment and the protection of Plaintiffs and Class Members' Private Information were material aspects of these express contracts.

224. The express contracts for the provision of educational services and employment – contracts that include the contractual obligations to maintain the privacy of Plaintiffs and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.

225. At all relevant times, Defendant expressly represented in its Privacy Notice, among other things, that Plaintiffs and Class Members PII would, among other things to "is not released to external parties without your consent unless required by law."

226. Defendant's express representations, including, but not limited to, express representations found in its Privacy Notice, formed and embodied an express contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs and Class Members' Private Information.

227. Plaintiffs and Class Members value their privacy, the privacy of their dependents, and the ability to keep their Private Information. Plaintiffs and Class Members would not have entered into these contracts with Defendant without an understanding that its Private Information would be safeguarded and protected.

228. A meeting of the minds occurred, as Plaintiffs and Members of the Class agreed to and did provide their Private Information to Defendant and paid for the educational services or provided their labor in exchange for, amongst other things, both the provision of educational services and employment and the protection of its Private Information.

229. Plaintiffs and Class Members performed their obligations under the contract when they paid for its educational services, submitted their applications or provided their labor and provided their Private Information.

230. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

231. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiffs and Class Members' Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and more than seven million Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like MGDPA and Section 5 of the FTCA, or otherwise protect Plaintiffs and the Class Members' Private Information, as set forth above.

232. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

233. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Members of the Class did not receive the full benefit of the bargain, and instead received educational services, employment and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the educational services and employment with data security protection they paid for and the healthcare they received.

234. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have provided their information to Defendant.

235. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries,

including without limitation the release, disclosure, and publication of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of its educational services and employment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

236. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, respectfully requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment.

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: October 9, 2023

Respectfully Submitted,

/s/ Stuart L. Goldenberg
Stuart L. Goldenberg (MN #0158719)
Noah C. Lauricella (MN #397896)
Ethan Adams (MN #0401141)
GoldenbergLaw, PLLC
800 LaSalle Ave, Suite 2150
Minneapolis, MN 55402
slgoldenberg@goldenberglaw.com
nlauricella@goldenberglaw.com
eadams@goldenberglaw.com

By: */s/ David S. Almeida*

David S. Almeida*
Matthew J. Langley*
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
(312) 576-3024
david@almeidalawgroup.com
matt@almeidalawgroup.com

**Pro Hac Vice* to Be Filed

COUNSEL FOR PLAINTIFFS & THE CLASS

ClassAction.org
