UNITED STATED DISTRICT COURT
DISTRICT OF MINNESOTA

Jasmyn Martin, individually and on behalf of herself and all others similarly situated, Plaintiff, v. University of Minnesota, Defendant.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Jasmyn Martin (hereinafter, "Plaintiff" or "Plaintiff Martin"), by her undersigned counsel, files this Class Action Complaint on behalf of herself and a class of all similarly situated persons against Defendant University of Minnesota ("UMN" or "Defendant"). Plaintiff bases the forgoing allegations upon personal information and belief, the investigation of counsel, and states as follows:

INTRODUCTION

1. On August 22, 2023, the University of Minnesota sent an email to all faculty, staff, and students informing them that "On July 21, 2023, the University became aware that an unauthorized party claimed to be in possession of sensitive data allegedly taken from the University's systems. As soon as the claim was discovered, we initiated an investigation and promptly retained outside global forensics professionals to help determine the validity of the party's claims and to ensure the security of the University's systems." Despite having

been aware of the fact that an unauthorized party had taken its data (the "Data Breach"), UMN waited a full month to inform faculty, staff and students, and even the email sent did not constitute notice of the breach. Instead, UMN noted "To the extent any sensitive personal data was improperly accessed, we will notify affected individuals and provide resources to help protect against misuse of their information, as required by federal and state law, University policies, and in accordance with our obligations to the University community. The University has already notified state and federal regulatory agencies, as required by law."

2. UMN's disclosure of the Data Breach comes nearly a month after a tech blog, thecyberexpress.com, reported on a potential UMN data breach in July. That blogger reported that "in a July 15th post on the dark web, a hacker claimed to have accessed the University of Minnesota data warehouse containing records since 1989 and extracted information including 7 million unique social security numbers."[1]

3. UMN is a public research university with multiple campuses throughout the State of Minnesota. UMN is the oldest and largest in the University of Minnesota system and has the ninth-largest main campus student body in the United States, with more than 50,000 students annually. UMN claims to have "50,000+" students and "485,000" living

[1] *See* Dana Thiede & Lou Raguse, "U of M Investigating Claimed Data Breach," Kare11 News (Aug, 22, 2023), *available at* https://www.kare11.com/article/news/local/u-of-m-investigating-claimed-data-breach/89-17a1736f-a704-4495-9337-079e0c77ccd5 (last accessed Aug. 29, 2023).

alumni.[2] UMN claims to be "[a]n [i]ndispensable [e]ngine for Minnesota" that "contributes more than $8.6 billion a year in economic activity to the state.[3]

4. Students, employees, applicants, and others affiliated with the UMN provide it with highly sensitive personal information, including Personally Identifying Information ("PII") including, among other things, names, addresses, telephone numbers, email addresses, and social security numbers. UMN gathers this information and stores it on its servers in a database.

5. This type of personal and sensitive data is highly targeted by hackers who seek to exploit this data for nefarious purposes. Indeed, PII and, in particular, Social Security numbers, have inherent value, and are routinely marketed and sold on the dark web. In the wrong hands, the personal and sensitive data that UMN collects and stores may be utilized to cause significant harm to the those who provided this information, including being used to orchestrate a swath of fraudulent schemes.

6. The value of this information on the dark web is well recognized in the modern data economy, and the foreseeable risk to customers' identities as a result of a criminal hacking event is known and recognized by technology companies that gather and store data, including Defendant.

7. UMN gathers, stores, and uses sensitive information it gathers from students, applicants, employees, and other individuals, including social security numbers. As such, UMN has a duty to protect the sensitive data it chooses to store. UMN recognizes the

[2] *About Us*, UMN (last visited, Aug. 29, 2023), https://twin-cities.umn.edu/about-us
[3] *Id.*

importance of protecting this data. Indeed, it admits to being governed by the Minnesota Government Data Practices Act and cannot release personally identifying information without consent.[4] UMN has also implemented policies and procedures regarding its expected behavior in the case of a "Data Security Breach," which states that it "will provide timely and appropriate notice to affected individuals when there has been a breach of security involving private data about them."[5] Further, under Minn. Stat. § 13.05, subd. 5(2) of the Minnesota Government Data Practices Act, 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."

8. Despite these requirements and its understanding of the need to implement reasonable security measures to keep students and employees' information 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 security numbers. The stolen information includes data from digitized records initially created as far back as 1989.

9. It appears UMN did not learn that the hacker had infiltrated its systems, gained control over them, and stole millions of social security numbers until after the hacker had successfully infiltrated its system and exfiltrated millions of individuals' data. Indeed,

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

[5] *See* https://policy.umn.edu/it/securitybreach (last accessed Aug, 29, 2023).

UMN only just 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.

10. Despite this knowledge and investigation, UMN has not timely notified Plaintiff or the Class, sending vague emails promising that notice will be sent later instead.

11. The Data Breach has already had serious consequences and will continue to do so. As a direct and proximate result of UMN's inadequate data security and the resulting data breach, Plaintiff and the Class have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including: (i) from the untimely and inadequate notification of the Data Breach, (ii) the diminished value of their personal information; (iii) the resulting immediate and continuing risk of future ascertainable losses, economic damages and other actual injury and harm, (iv) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; (v) out-of-pocket expenses for securing identity theft protection and other similar necessary services; and (iv) emotional harm and distress from the exposure of their sensitive records and the prolonged and heightened risk of harm.

12. Plaintiff, therefore, brings this Class Action Complaint seeking relief for her injuries and those of persons who were similarly impacted by the Data Breach and inadequate data security.

PARTIES

13. Plaintiff Jasmyn Martin is a citizen of Minnesota residing in Brooklyn Park, Minnesota. Plaintiff Martin applied to attend school as an undergraduate at the UMN in 2016. In her application, she provided UMN with her PII, including her name, contact information, social security number, and date of birth, among other information. She was accepted to the UMN and attended from 2017 to 2019. Additionally, separate and apart from her UMN application, Plaintiff Martin was required to provide her medical records and bank account information in order to receive scholarship funds.

14. Defendant University of Minnesota, or UMN, is a higher education public institution in the State of Minnesota that accepts applicants to its undergraduate and graduate programs from people throughout the United States and from non-U.S. born individuals. It, furthermore, employs thousands of staff in academic and non-academic roles.

JURISDICTION

15. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, minimal diversity is met under CAFA because at least one member of the proposed Class is diverse from the Defendant. UMN is located and operates exclusively in the State of Minnesota and is a citizen of only that State. The Class is comprised of

applicants to attend UMN, and current and former students and employees of UMN, which includes individuals dispersed throughout the country and who are citizens of States other than Minnesota. Plaintiff alleges that, in the aggregate, the claims of all putative class members exceed $5,000,000, exclusive of interest and costs.

16. This Court has general personal jurisdiction over UMN because UMN is located entirely within the State of Minnesota, and is a Minnesota public institution operating on behalf of the State of Minnesota. UMN has minimum contacts with Minnesota because it is located there and conducts substantial business there, and Plaintiff's claims arise from UMN's conduct in Minnesota, including because UMN's database containing the information stolen is located in Minnesota.

17. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in Minnesota and because UMN conducts a substantial part of its business within this District.

BACKGROUND

A. UMN Collects Personal and Sensitive Information from Students, Employees, Applicants and Others

18. UMN is one of the nation's premier public higher education institutions. Annually, it accepts thousands of applicants into its undergraduate and graduate programs. It, furthermore, employes thousands of employees to maintain its operations. As of 2022, UMN employed 4,033 academic staff, over 24,000 staff in general, and had nearly 55,000

students, including 30,560 undergraduates, 11,613 postgraduates, and 3,875 doctoral students.

19. 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, along with a myriad of additional personal, identifying information.

20. Each year, UMN receives tens of thousands of applicants and employes tens of thousands of academic and non-academic staff. Consequently, the UMN has built up a massive repository of sensitive information on millions of individuals.

21. UMN understands the importance of securing the highly sensitive PII that it collects and stores in its database. UMN, as a public institution, is governed by the Minnesota Government Data Practices Act ("MGDPA"), Minn. Stat. § 13, *et seq.* 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 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).

22. 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.

23. Furthermore, the MGDPA required UMN to conduct 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).

24. 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.[6]

25. Indeed, UMN has implemented a Data Security Breach policy that states that "The University will provide timely and appropriate notice to affected individuals when there has been a breach of security involving private data about them."[7] Under that policy,

[6] *See supra* note 4.
[7] *See supra* note 5.

the data practices compliance official appears to be the Chief Information Security Officer. "The Chief Information Security Officer (CISO), in consultation with the Office of the General Counsel and appropriate privacy officers, is responsible for determining whether a breach of information security or University private data has occurred and whether notification to affected individuals is required. The CISO may also seek advice from other key administrators responsible for security and privacy at the University and consult with responsible administrators in the affected campus, area, or unit."[8]

26. In fact, in its FAQ section describing what to do in the case of a data breach and explaining the purposes of the policy, UMN identifies the scenarios it actually experienced as suspected data breaches and notes that "These are examples of suspected electronic breaches of University private data: a device storing or accessing University private data has been accessed by an unauthorized party, electronic files have been mistakenly posted on the web or e-mailed to the wrong recipients, or a laptop, tablet, smartphone, or other electronic storage device has been stolen or lost."[9]

27. Despite its knowledge, UMN failed to enact measures sufficient to protect against the Data Breach, given that a hacker released millions of Social Security numbers and other PII stolen from a UMN database in July 2023.

[8] *Id.*

[9] *See* https://policy.umn.edu/it/securitybreach-faq01 (last accessed Aug. 29, 2023).

B. UMN's Inadequate Data Security Measures Exposed Plaintiff's and the Class's PII

28. On August 22, 2023, the University of Minnesota confirmed that it had contacted law enforcement concerning a potential data breach that it became aware of on July 21, 2023.[10] Specifically, representatives of the UMN stated that they became aware that an "unauthorized party" had claimed to possess sensitive data taken from the UMN's computer systems.[11]

29. After confirming the investigation to the press, the UMN Office of Information Technology, in an email signed by Bernard Gulachek, Vice President and Chief Information Officer, and Brian Dahlin, Chief Information Security Officer, sent a University-wide email confirming the investigation. That email read, in full:

> Dear faculty, staff, and students,
>
> We're writing today to make you aware of a data security issue. On July 21, 2023, the University became aware that an unauthorized party claimed to be in possession of sensitive data allegedly taken from the University's systems. As soon as the claim was discovered, we initiated an investigation and promptly retained outside global forensics professionals to help determine the validity of the party's claims and to ensure the security of the University's systems. We have also been in regular contact with law enforcement and will continue to cooperate in any active investigation.
>
> To the extent any sensitive personal data was improperly accessed, we will notify affected individuals and provide resources to help protect against misuse of their information, as required by federal and state law, University policies, and in accordance with our obligations to the University community. The University has already notified state and federal regulatory agencies, as required by law.
>
> The safety and privacy of all members of the University community are among the University's top priorities. We investigate these situations

[10] *See supra* note 1.
[11] *Id.*

immediately and fully, and are committed to keeping the community informed as additional, relevant information becomes available.

Sincerely,
Bernard Gulachek
Vice President and Chief Information Officer

Brian Dahlin
Chief Information Security Officer

30. The UMN became aware of the data breach from disclosures made by the purported hacker. On July 15, 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 7 million unique individuals.[12] According to an article posted about the hack on July 21, 2023, 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.[13]

31. The leaked information on the dark web reportedly listed in two tables, one named "PS DIVERSITY", concerning diversity statistics, and another named "PS_DWAD_APPL_DATA_HS", which involves admission statistics.[14] Although the scope of the data breach is not clear, the data of those applying to be admitted to UMN is included in the PS_DWAD_APPL_DATA_HS table, indicating tens if not hundreds of thousands of individuals have had their data stolen and posted to the dark web.

[12] https://thecyberexpress.com/university-of-minnesota-data-breach/
[13] *Id.*
[14] *Id.*

32. Moreover, 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[.]"[15]

33. 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 name.[16] Lanterman also noted that "The breach serves as a stark reminder of the importance of data security and the measures institutions need to adopt in today's interconnected environment."[17]

34. According to the UMN, they have run scans that have indicated that no additional suspicious activity is ongoing.[18] Thus, the hacker successfully entered into the UMN's networks, gained access to the UMN's database, exfiltrated a significant sum of data, including PII and social security numbers, all without detection by the UMN or any of its security tools or personnel. Indeed, the UMN only became aware of the attack after the hacker publicly described it and posted the stolen data.

35. UMN has known of the Data Breach since at least July 21, 2022, but has yet to formally notify and current or past staff, students, applicants, or faculty..

---

[15] *See supra* note 1.

[16] *Id.*

[17] *See* Mark Lanterman, LinkedIn (Aug, 24, 2023), https://www.linkedin.com/posts/marklanterman_u-of-m-investigating-data-breach-scope-of-activity-7100177040938594304-9gmB/ (last accessed Aug, 29, 2023).

[18] Matt Sepic, "University of Minnesota Investigating Claims of Big Data Breach," MPRNews (Aug. 22, 2023), *available at* https://www.mprnews.org/story/2023/08/22/university-of-minnesota-investigating-claims-of-big-data-breach (last accessed Aug. 29, 2023).

C. UMN's Data Breach Caused Plaintiff's and the Class's Injuries

36. UMN's Data Breach resulted in the theft and exposure of confidential data, including Social Security numbers and other PII. The full extent of the data compromised is not yet known, but given the vast stores of information that defendant maintains, it is likely to include additional confidential data, including addresses, passport numbers, driver's license numbers, work documents, tax and financial documents, grade and schedule information, and potentially health information. Exposure of this type of data puts individuals at a significant and prolonged risk of fraud and identity theft. Indeed, personal information like that stolen from UMN is valuable and has been commoditized in recent years because of its use in conducting identity theft and fraud.

37. After a data breach like UMN's, 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 personally identifying information to create fake IDs, make fraudulent transactions, obtain loans or commit other acts of identity theft.[19]

38. Federal and state governments established security standards and issued recommendations to minimize unauthorized data disclosures, and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses highlighting 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.

[19] *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/

39. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for businesses and other entities that maintain PII. Among other things, the guidelines note entities should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend 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.

40. The FTC recommends that entities not maintain PI 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.

41. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against entities for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

42. Failing to take basic security measures in designing and implementing their computer systems and employee requirements and securing Plaintiff's and Class Members' PII, Defendant allowed unauthorized third parties and potentially thieves to access and collect individuals' PII. Defendant failed to employ reasonable and appropriate measures to protect against unauthorized disclosure and access to Plaintiff's and Class Members' PII. Defendant's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

43. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data. The body of law created by the FTC recognizes that failure to restrict access to information and failure to segregate access to information may violate the FTC Act.

44. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data, including driver's license numbers and other motor vehicle records (i.e., PI) constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

45. The PII of consumers and educational entity participants, such as Plaintiff and the Class, is valuable and has been commoditized in recent years.

46. The ramifications of Defendant's failure to keep Plaintiff's and Class members' PII secure are severe. Identity theft occurs when someone uses another's personal and

financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

47. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

48. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity. Here, the hacker explicitly noted that the information is now available on the dark web.]

49. Once PII 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 lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

50. 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 individuals and business victims.

51. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not

rapidly report—and still has not reported or sent notice—to Plaintiff and Class members that their PII has been stolen.

52. 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.

53. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

54. 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.

55. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, 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 their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

56. 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, Plaintiff and

Class members will need to be remain vigilant against unauthorized data use for years or even decades to come.

57. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point: Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.

58. 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.[20] 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 unapproved activity; (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.[21]

59. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. See *In the matter of Lookout Services*, Inc., No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass

[20] *Start With Security, A Guide for Business*, FTC (last visited Sept. 22, 2021), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[21] *Id.*

authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); In the matter of The TJX Cos., Inc., No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded UMN's Data Breach, further clarify the measures businesses must take to meet their data security obligations.

60. Consumers place a high value on their PII and a greater value on their PHI, in addition to the privacy of their personal information. Research shows how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US $30.49–44.62."[22]

[22] Il-Horn Hann et al., *The Value of Online Information Privacy* (Oct. 2002) available at http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Sept. 22, 2021); *see*

61. By virtue of the Data Breach here and unauthorized release and disclosure of the PII of Plaintiff and the Class, UMN deprived Plaintiff and the Class of the substantial value of their personal information, to which they are entitled. As previously alleged, UMN failed to provide reasonable and adequate data security, pursuant to and in compliance with industry standards and applicable law.

62. As a direct and proximate result of UMN's wrongful actions and omissions here, Plaintiff and the Class have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including: (i) the resulting immediate and continuing risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; (iii) out-of-pocket expenses for securing identity theft protection and other similar necessary services; (iv) the dimiunition in value of their social security numbers and other private information, the value of which is derived from its confidentiality and privacy; and (v) emotional distress caused by the impending risk of fraud and identity theft and the loss of privacy, confidentiality, and value of their personal information.

also Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22 (2) Information Systems Research 254, 254 (June 2011).

CLASS ALLEGATIONS

63. Plaintiff brings this nationwide class action on behalf of herself and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure.

64. The Nationwide Class that Plaintiff seeks to represent is defined as follows: All individuals whose PII was compromised from UMN during its Data Breach announced publicly by UMN on August 22, 2023.

65. 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 has 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 their 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 their immediate family members.

66. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

67. **Numerosity.** Members of the proposed Class likely number in at least the hundreds of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

68. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant's inadequate data security measures were a cause of the Data Breach;

c. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII;

d. Whether Defendant allowed the compromise of PII obtained from the records of Defendant or third parties without the permission or consent of Plaintiff and the Class;

e. Whether Plaintiff and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Defendant violated Minnesota statutes or common law requirements;

g. Whether Plaintiff and the Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

h. Whether Plaintiff and the Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

69. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved predominate over any individualized issues. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

70. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. All Class Members were subject to the Data Breach and had their PII accessed by, used and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class Members in the same manner.

71. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class Members they seek to represent; they retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

72. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the Class Members pale compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class Members to

individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase 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 single adjudication, economies of scale, and comprehensive supervision by a single court.

73. **Injunctive and Declaratory Relief:** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because Defendant, through its uniform conduct, acted or failed and 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. Moreover, Defendant continues to maintain inadequate security practices, retain possession of Plaintiff's and Class Members' PII, and has not been forced to change its practices or relinquish PII by nature of other civil suits or government enforcement actions, thus making injunctive relief a live issue and appropriate to the Class as a whole.

74. Likewise, particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. whether Plaintiff's and Class Members' PII was accessed and/or acquired by an unauthorized party because of the data security breach;

b. whether Defendant owed a legal duty to Plaintiff and Class Members;

c. whether Defendant's actions were knowing in improperly disclosing driver's license numbers to unauthorized parties and/or entities;

d. whether Defendant failed to take adequate and reasonable steps to safeguard Plaintiff's and Class Members' PII;

e. whether Defendant failed to adequately monitor their data security systems;

f. whether Defendant failed to comply with applicable laws, regulations, and/or industry standards relating to data security amounting to negligence;

g. whether Defendant's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

h. whether Defendant knew or should have known it did not employ adequate and reasonable measures to keep Plaintiff's and Class Members' PII secure; and

i. whether Defendant's failure to adhere to FTC data security obligations, industry standards, and/or measures recommended by data security experts caused the Data Breach.

LEGAL CLAIMS

COUNT I

Negligence
(On behalf of the Nationwide Class)

75. Plaintiff repeats and re-alleges the allegations contained in the preceding paragraphs as if fully set forth herein.

76. UMN owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the sensitive data it solicited from Plaintiff and the Class, managed and stored. This duty arises from multiple sources.

77. UMN owed a common law duty to Plaintiff and the Class to implement reasonable data security measures because it was foreseeable that hackers would target UMN's databases because it contained millions of individuals' valuable PII and, UMN further knew that, should a breach occur, Plaintiff and the Class would be harmed. UMN alone controlled its technology, infrastructure, digital platforms, and cybersecurity that were exposed during the Data Breach and allowed hackers to breach and steal information from its database. It further knew or should have known that if hackers breached its data systems, they would extract sensitive data and inflict injury upon Plaintiff and the Class. UMN knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and stolen, and that individual need would continue long after the Data Breach ended. Therefore, the Data Breach, and the harm it caused Plaintiff

and the Class, was the foreseeable consequence of UMN's unsecured, unreasonable data security measures.

78. UMN, furthermore, assumed a duty to protect individuals' data by soliciting sensitive PII, collecting that data, and storing that data in its own databases. In fact, Plaintiff and the Class were required to provide social security numbers and other PII in order to obtain employment or apply to attend UMN. UMN was the only entity capable of implementing reasonable measures to protect Plaintiff and the Class's sensitive data.

79. Additionally, Section 5 of the FTC Act, 15 U.S.C. § 45, required UMN to take reasonable measures to protect Plaintiff and the Class's sensitive data and is a further source of UMN's duty to Plaintiff and the Class. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by entities like UMN of failing to implement and use reasonable measures to protect sensitive data. UMN, therefore, was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of UMN's duty to adequately protect sensitive information. By failing to implement and use reasonable data security measures, UMN acted in violation of § 5 of the FTC ACT.

80. UMN is obligated to perform its business operations in accordance with industry standards. Industry standards are another source of duty and obligations requiring UMN to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff

and the Class. Industry best practices put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, UMN was the only entity capable of adequately protecting the data that it alone solicited, collected, and stored.

81. UMN breached its duty to Plaintiff and the Class by implementing unreasonable data security measures that it knew or should have known could cause a Data Breach. UMN recognized the need to keep PII confidential and safe from cybercriminals who targeted it. Despite that, UMN implemented unreasonable data security that allowed a single hacker to breach its systems, gain control over them, access its database, and exfiltrate data on millions of individuals, all undetected.

82. UMN was fully capable of preventing the Data Breach. UMN is a sophisticated entity that accounts for one of the most respected public higher education entity in the world. It knew or should have known of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented and used, would have prevented the Data Breach from occurring at all, or limited and shortened the scope of the Data Breach. UMN thus failed to take reasonable measures to secure its system, leaving it vulnerable to a breach

83. As a direct and proximate result of UMN's negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including the ongoing risk that their data

will be used nefariously against them or for fraudulent purposes. Plaintiff, therefore, seeks all remedies available under the law for UMN's negligence.

COUNT II

Negligence *Per Se* (On behalf of the Nationwide Class)

84. Plaintiff repeats and re-alleges the allegations contained in the preceding paragraphs as if fully set forth herein.

85. UMN's unreasonable data security measures and failure to timely notify Plaintiff and the Class of the Data Breach violates Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, both require businesses to institute reasonable data security measures and breach notification procedures, which UMN failed to do.

86. Section 5 of the FTC Act, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities like UMN of failing to implement and use reasonable measures to protect individuals' sensitive data. The FTC publications and orders described above also form the basis of UMN's duty.

87. 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).

88. UMN violated Section 5 of the FTC Act and the MGDPA by failing to use reasonable measures to protect Plaintiff 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.

89. UMN's violation of Section 5 of the FTC Act and the MGPDA each separately constitute negligence per se.

90. Plaintiff and the Class are within the class of persons Section 5 of the FTC Act (and similar state statutes) and the MGDPA were intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) and the MGPDA were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class.

91. As a direct and proximate result of UMN's negligence *per se*, Plaintiff and the Class have suffered and continue to suffer injury. Plaintiff, therefore, seeks all remedies available under the law for UMN's negligence *per se*.

COUNT III

Violation of Minnesota Government Data Practices Act, Minn. Stat. § 13, *et seq*.
(On behalf of the Nationwide Class)

92. Plaintiff repeats and re-alleges the allegations contained in the preceding paragraphs as if fully set forth herein.

93. 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 attorneys fees." Minn. Stat. § 13.08, subd. 1. 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.

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

95. 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).

96. 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).

97. 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.[23] UMN acknowledged this obligation in the letter it sent faculty, staff and students on August 22, 2023, noting "To the extent any sensitive personal data was improperly accessed, we will notify affected individuals and provide resources to help protect against misuse of their information, as required by federal and state law, University policies, and in accordance with our obligations to the University community. The University has already notified state and federal regulatory agencies, as required by law. The safety and privacy of all members of the University community are among the University's top

[23] *See supra* notes 4 and 5.

priorities. We investigate these situations immediately and fully, and are committed to keeping the community informed as additional, relevant information becomes available."

98. However, UMN failed to adopt "appropriate security safeguards" to protect Plaintiff and the Class's highly sensitive information that it stored in its database, which is clear based on the way in which the Data Breach occurred. 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. The hacker exfiltrated records going back to 1989, all of which were apparently stored together. 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.

99. UMN's conduct violates the MGDPA. In addition, Plaintiff and the Class suffered damages 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.

100. Specifically, Plaintiff 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 Plaintiff's and the Class's identities. Plaintiff

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. Plaintiff, 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, Plaintiff suffered emotional distress stemming from the disclosure of her sensitive data and the heightened and prolonged risk of harm she now suffers.

101. Plaintiff, therefore, seeks to recover the damages she suffered and costs and attorneys' fees.

COUNT IV

Invasion of Privacy
(On behalf of the Nationwide Class)

102. Plaintiff repeats and re-alleges the allegations contained in the preceding paragraphs as if fully set forth herein.

103. Plaintiff and Class Members had a legitimate expectation of privacy with respect to their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

104. Defendant owed a duty to students, faculty and staff, along with UMN applicants, including Plaintiff and Class Members, to keep their PII contained as a part thereof, confidential.

105. The unauthorized release of PII, especially the breadth of information available here, is highly offensive to a reasonable person.

106. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as part of their application, work, and education at UMN but privately, with the intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

108. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate and knew that it had federal, state and common law duties to secure the trove of PII it maintains.

109. Acting with knowledge, UMN had notice and knew, or had constructive knowledge, that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

110. As a proximate result of Defendant's acts and omissions, Plaintiff's and Class Members' PII was disclosed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

111. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class

Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons.

112. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

COUNT V

Declaratory Judgment
(On behalf of the Nationwide Class)

113. Plaintiff repeats and re-alleges the allegations contained in the preceding paragraphs as if fully set forth herein.

114. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

115. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges UMN's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

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

a. UMN owed, and continues to owe a legal duty to secure the PII with which it is entrusted, and to notify impacted individuals of the Data Breach under the common law, the MGDPA, and Section 5 of the FTC Act;

b. UMN breached, and continues to breach, its legal duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. UMN's breach of its legal duty continues to cause harm to Plaintiff and the Class.

117. The Court should also issue corresponding injunctive relief requiring UMN to employ adequate security protocols consistent with industry standards to protect Plaintiff's and the Class's data and PII.

118. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of UMN's data systems. If another breach of UMN's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable,

do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

119. An additional data breach at UMN is likely given that UMN has conceded that it suffered a previous data breach in 2021 that did not prevent the Data Breach from occurring and that its changes in the wake of the 2021 breach did not prevent the Data Breach.

120. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to UMN if an injunction is issued.

121. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

122. Wherefore, Plaintiff, on behalf of herself and the Class, requests that this Court award relief as follows:

a. An order certifying the class and designating Plaintiff as the Class Representative and her counsel as Class Counsel;

b. An award to Plaintiff and the proposed Class members of damages with pre-judgment and post-judgment interest;

c. A declaratory judgment in favor of Plaintiff and the Class;

d. Declaratory and Injunctive relief to Plaintiff and the Class;

e. An award of attorneys' fees and costs pursuant to the MGPDA and as otherwise allowed by law; and

f. An award such other and further relief as the Court may deem just and proper, necessary or appropriate.

JURY TRIAL DEMANDED

123. Plaintiff hereby demands a jury trial for all the claims so triable.

Dated: August 29, 2023

Respectfully,

s/ Kate M. Baxter-Kauf
Karen Hanson Riebel
Kate M. Baxter-Kauf
Carey R. Johnson
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South
Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com
crjohnson@locklaw.com

Jon Tostrud (MN Bar No. 0251768)
Anthony Carter (*pro hac vice forthcoming*)
TOSTRUD LAW GROUP, P.C.
1925 Century Park East
Suite 2100
Los Angeles, CA 90067
Telephone: (310) 278-2600
Facsimile: (310) 278-2640

Blaine Finley (p*ro hac vice forthcoming*)
CUNEO GILBERT & LADUCA, LLP

4725 Wisconsin Ave. NW
Suite 200
Washington, DC 20016
Telephone: (202) 789-3960
Facsimile: (202) 589-1813
bfinley@cuneolaw.com
Attorneys for Plaintiff and Proposed Class