UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

YERVANT DERMENJIAN, individually and on behalf of all others similarly situated, Plaintiff, v. CARNEGIE MELLON UNIVERSITY, Defendant.	Case No. 2:25-cv-00459 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Yervant Dermenjian ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Carnegie Mellon University ("Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. Defendant is a private research university located in Pittsburgh, Pennsylvania. Defendant consists of the undergraduate Dietrich College of Humanities and Social Sciences, the College of Engineering, the School of Computer Science, the Tepper School of Business, the College of Fine Arts, the Mellon College of Science, the Heinz College of Information Systems and Public Policy, and various graduate and professional programs.[1]

[1] https://www.cmu.edu/about/

2. In order to provide services to its students, Defendant acquires, stores, processes, analyzes, and otherwise utilizes Plaintiff's and Class Members' personally identifiable information, including, but not limited to, first and last name, Social Security number, student identification number, date of birth, passport number, and health information. ("Private Information" or "PII").

3. On August 25, 2023, Defendant experienced a data security incident where unauthorized cybercriminals accessed Defendant's information systems and databases (the "Data Breach"). Defendant launched a forensic investigation that "the information that was accessed may have contained your name, social security number and/or date of birth." [2]

4. Through the cyber-attack, criminal cyberthieves accessed and exfiltrated Plaintiff's and Class Members' Private Information.

5. Based upon the investigation, more than 7,343 individuals' Private Information was affected in the Data Breach. [3]

6. Despite becoming certain of the Data Breach on or around December 04, 2023, Defendant did not notify Plaintiff and other Class Members until on or around January 12, 2024 ("Notice of Data Breach").

7. As a result of the Data Breach, Plaintiff and Class Members suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss

[2] *See* Sample Data Breach Notice Letter, https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/a3149073-c145-4b26-ae92-a062ca803d41/715559d7-13dd-472f-ba05-4361edacd1e5/EXPERIAN_K6458_Carnegie%20Mellon%20University_L01_SAS_2.pdf (last visited: January 23, 2025).
[3] *Id*.

of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably incurred to remedy or mitigate the effects of the attack, and the loss of, and diminution in, value of their personal information.

8. In addition, Plaintiff's and Class Members' sensitive confidential Private Information was compromised and unlawfully accessed due to the Data Breach. This information, while compromised and taken by unauthorized third parties, remains also in the possession of Defendant, and without additional safeguards and independent review and oversight, remains vulnerable to additional hackers and theft.

9. Particularly alarming is the fact that the Private Information compromised in the Data Breach included Social Security numbers, which are durable and difficult to change.

10. Defendant did not notify Plaintiff and Class Members that their Private Information was subject to unauthorized access resulting from the Data Breach until on or around January 12, 2024, approximately 5 months after the Data Breach was suspected.

11. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's and Class Members' Private Information.

12. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party.

13. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks and ransomware malware.

14. The mechanism of the hacking and potential for improper disclosure of Private Information was a known risk to Defendant and entities like it, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition and vulnerable to theft.

15. Defendant disregarded the rights of Plaintiff and Class Members by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard their patient's Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members prompt notice of the Data Breach.

16. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their respective lifetimes.

17. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining

driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

18. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

19. By waiting to notify Plaintiff and Class Members, Defendant harmed Plaintiff and Class Members. Said differently, if Defendant had notified Plaintiff and Class Members at or around the time the Data Breach was first discovered, Plaintiff and Class Members would be in a better position to protect themselves.

20. Even though Defendant has offered credit monitoring services for a short period of time, Plaintiff and Class Members will incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft beyond the services offered by Defendant.[4]

21. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

22. Plaintiff seeks remedies including, but not limited to, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

23. Plaintiff also seeks injunctive and equitable relief to prevent future injury on behalf of himself and the putative Class.

[4] Defendant has provided Plaintiff with a complimentary 24-month membership in Experian Identity Works.

PARTIES

24. Plaintiff Yervant Dermenjian is, and at all times mentioned herein was, an individual citizen of the State of New Jersey, residing in Roseland, New Jersey. Plaintiff received a Notice of Data Breach from Defendant dated January 12, 2024.

25. Defendant Carnegie Mellon University is a nonprofit corporation incorporated under the laws of the State of Pennsylvania with its principal place of business at 5000 Forbes Avenue, Pittsburgh, Pennsylvania, 15213.

JURISDICTION AND VENUE

26. This Court has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in Pennsylvania and this District through its headquarters, offices, parents, and affiliates.

27. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000 exclusive of interest and costs; there are more than 100 members in the proposed class; and at least one member of the class, including the Plaintiff, are citizens of a state different from Defendant.

28. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

DEFENDANT'S BUSINESS

29. Defendant is a private university based in Pittsburgh. [5]

30. Defendant obtained the Private Information of Plaintiff and Class Members as part of the process of providing educational services, as well as attendant aspects of running an educational institution, such as providing health services, counseling, technological services and financial aid services.

31. In addition to tuition and other revenue that Defendant receives from its students, Defendant charges a "Technology Fee" of $470, part of which is presumably dedicated to establishing and maintaining the data security for the network infrastructure that houses Plaintiff's and Class Members' Private information.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

33. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Defendant failed to implement industry standard protections for that sensitive information.

34. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

[5] https://www.cmu.edu/about/

THE ATTACK AND DATA BREACH

35. On or about August 25, 2023, Defendant suspected a possible data security incident that impacted its computer networks. [6]

36. Defendant did not notify those it determined were affected until over 6 months had passed.

37. Through the cyber-attack, Plaintiff's and Class Members' Private Information, including their names, Social Security numbers, and dates of birth, were accessed and exfiltrated by criminal third-parties.

38. Based on its investigation, Defendant admits that Plaintiff's and Class Members' Private Information was accessed and exfiltrated via a cyber-attack conducted by cybercriminals.

39. On information and belief, the Private Information accessed by hackers was not encrypted.

40. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of persons such as Plaintiff and the Class Members.

41. Due to Defendant's inadequate security measures, Plaintiff and the Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

42. Due to Defendant's inadequate security measures, Plaintiff's and Class Members' Private Information is now in the hands of cyberthieves.

---

[6] *See* Notice of Data Breach Letter, https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/a3149073-c145-4b26-ae92-a062ca803d41/715559d7-13dd-472f-ba05-4361edacd1e5/EXPERIAN_K6458_Carnegie%20Mellon%20University_L01_SAS_2.pdf

43. Defendant failed to comply with its obligations to keep such information confidential and secure from unauthorized access, as well as its obligation to timely notify Plaintiff and Class Members.

THE DATA BREACH WAS FORSEEABLE

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

45. In July 2022, a survey was published by Sophos detailing findings regarding the impact of ransomware on educational institutions in 31 countries throughout the world, finding that educational institutions were being attacked at a higher rate than other sectors, that the results were more devastating, and the recovery period longer than other sectors subject to ransomware attacks.[7]

46. In 2021, the FBI's Cyber Division published an advisory notice warning about ransomware attacks targeting colleges and universities.[8]

47. As one cybersecurity executive stated, "They're juicy targets because they have student data, they have research information and they have critical operations that need to operate on a very strict timeline," Louie said. "They can be exploited on many fronts."[9] Furthermore, "In ransomware attacks on colleges, there is the troubling potential for hackers to get their hands on

[7] https://www.sophos.com/en-us/press/press-releases/2022/07/ransomware-attacks-on-education-institutions-increase-sophos-survey-shows
[8] https://www.insidehighered.com/news/2021/03/19/targeting-colleges-and-other-educational-institutions-proving-be-good-business.
[9] *Id.*

very sensitive information such as medical histories or sexual assault complaints and use this against students."[10]

48. Educational institutions are likely to have financial information regarding its students, based on the financial aid programs that are nearly ubiquitous in the current world of higher education. Colleges and universities may also run medical or counseling clinics, with sensitive personal information.

49. Therefore, the increase in such attacks, and the attendant risk of future attacks in light of the nature of information under a university's care, was surely known to Defendant. Anyone in Defendant's industry knew or should have known of the risks of a ransomware attack and taken sufficient steps to fulfill its obligation to the people who entrust their personal data to the institution. Defendant failed to do so.

DEFENDANT FAILED TO PROPERLY PROTECT PLAINTIFF'S AND CLASS MEMBERS' PRIVATE INFORMATION

50. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted Private Information it was maintaining for Plaintiff and Class Members, causing the exposure of Private Information for more than 7,343 individuals.

51. In addition to the specific concerns in the educational sector, the FTC has promulgated numerous guides 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.

[10] *Id.*

52. 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 information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[11] 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.[12]

53. The FTC further recommends that companies not maintain Private Information 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.

54. Defendant failed to properly implement basic data security practices explained and set forth by the FTC.

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

---

[11] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 23, 2025).
[12] *Id*.

Defendant failed to comply with industry standards

56. Defendant did not utilize industry standards appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information for more than 7,343 individuals.

57. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against cyberattacks] and it is critical to take precautions for protection."[13]

58. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, 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 cyberattacks 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

[13] *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 visited Jan. 23, 2025).

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 cyberware 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.[14]

59. To prevent and detect cyber-attacks, including the 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

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

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)….

- **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….[15]

60. To prevent and detect cyberattacks, including the cyberattack 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;

[15] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited Jan. 23, 2025).

Thoroughly investigate and remediate alerts

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

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].[16]

61. As described above, experts studying cyber security routinely identify educational institutions as being particularly vulnerable to cyberattacks because of the value of the Private Information they collect and maintain.

[16] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Jan. 23, 2025).

62. Several best practices have been identified that at a minimum should be implemented by institutions such as Defendant, including, but not limited to, the following: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

63. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

64. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

65. Given that Defendant was storing the Private Information of thousands of individuals Defendant could and should have implemented all of the above measures to prevent cyberattacks.

66. The occurrence of the Data Brach 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 individuals' Private Information.

DEFENDANT'S BREACH

Defendant failed to properly protect Plaintiff's and Class Members' Private Information

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

a. Failing to maintain an adequate data security system to reduce the risk of data breaches, cyber-attacks, hacking incidents, and ransomware attacks;

b. Failing to adequately protect client's (students) Private Information;

c. Failing to properly monitor its own data security systems for existing or prior intrusions;

d. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

e. Failing to adhere to industry standards for cybersecurity.

68. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

69. Accordingly, as outlined below, Plaintiff and Class Members now face a present, increased, and immediate risk of fraud and identity theft.

Cyberattacks and data breaches cause disruption and put individuals at an increased risk of fraud and identity theft

70. 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 their good name and credit record."[17]

71. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, 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 otherwise harass or track the victim. 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. Here, the cyberthieves already have the Social Security numbers.

72. The FTC recommends that identity theft victims take several steps to protect their 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 their identity), reviewing their credit reports, contacting companies to remove fraudulent

[17] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[18]

73. The asset that is one's Private Information contains extremely valuable property rights.[19]

74. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

75. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

76. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at p. 29.

[18] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 23, 2025).

[19] See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *1 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

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

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

79. Thus, Plaintiff and Class Members must vigilantly monitor their financial profile for many years to come.

80. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[20]

81. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

82. 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. In addition, identity thieves may rent a house 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.

[20] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://www.infosecinstitute.com/resources/healthcare-information-security/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 23, 2025).

83. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[21] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file for unemployment benefits, or apply for a job using a false identity.[22]

84. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

85. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

86. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[23]

87. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card

[21] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 23, 2025).
[22] *Id* at 4.
[23] 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 Jan. 23, 2025).

information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[24]

88. For this reason, Defendant knew or should have known about these dangers and strengthened its network and data security systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Plaintiff Dermenjian's and Class Members' Harms and Damages

89. To date, Defendant has done little to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this data breach. Defendant's data breach notice letter completely downplays and disavows the theft of Plaintiff's and Class Members' Private Information, when the facts demonstrate that the Private Information was accessed and exfiltrated. The complimentary fraud and identity monitoring service offered by Defendant is wholly inadequate as the services are only offered for 24 months and it places the burden squarely on Plaintiff's and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

90. Plaintiff and Class Members have been injured and damaged by the compromise of their Private Information in the Data Breach.

91. Plaintiff's Private Information (including without limitation his name, date of birth, and Social Security number) was compromised in the Data Breach and is now in the hands of the

[24] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 23, 2025).

cybercriminals who accessed Defendant's network. Class Members' Private Information, as described above, was similarly compromised and is now in the hands of the same cyberthieves.

92. Plaintiff typically takes measures to protect his Private Information and is very careful about sharing his Private Information. Plaintiff has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

93. Plaintiff stores any documents containing his Private Information in a safe and secure location. Moreover, Plaintiff diligently chooses unique usernames and passwords for his online accounts.

94. To the best of his knowledge, Plaintiff's Private Information was never compromised in any other data breach.

95. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, and similar identity theft.

96. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

97. Plaintiff and Class Members will also incur out-of-pocket costs for protective measures such as credit monitoring fees (for any credit monitoring obtained in addition to or in lieu of the inadequate monitoring offered by Defendant), credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

98. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by the hacker and cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

99. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. In this case, Plaintiff and Class Members have actually paid a specific fee, a "Technology Fee" of $470 which presumably included the safeguarding of the Defendant's technology systems consistent with its policies and security requirements. Plaintiff and Class Members overpaid for these services that were intended to be accompanied by adequate data security, but were not.

100. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse. Indeed, Defendant's own notice of data breach provides instructions to Plaintiff and Class Members about all the time that they will need to spend to monitor their own accounts and statements received.

101. Plaintiff spent many hours over the course of several days attempting to verify the veracity of the notice of breach that he received and to monitor his financial and online accounts for evidence of fraudulent activities.

102. Plaintiff and Class Members have suffered actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Closely reviewing and monitoring Social Security Number, bank accounts, and credit reports for unauthorized activity for years to come.

103. Moreover, Plaintiff 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 sensitive and confidential personal, health, and/or financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

104. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

105. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at a present and imminent and increased risk of future harm.

CLASS REPRESENTATION ALLEGATIONS

106. Plaintiff brings this nationwide class action on behalf of himself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

107. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All United States residents whose Private Information was accessed or acquired during the data breach event that Defendant has stated commenced on or about August 25, 2023 (the "Nationwide Class").

108. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

109. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendant has identified thousands of individuals whose Private Information may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records. Defendant advised the Maine Attorneys General that the Data Breach affected more than 7,343 individuals.

110. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

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

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

c. Whether Defendant's data security systems prior to and during the hacking incident and Data Breach complied with applicable data security laws and regulations, *e.g.*, FTC Guidelines, HIPAA, etc.;

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

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

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

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

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

i. Whether Defendant owed a duty to provide Plaintiff and Class Members timely notice of this Data Breach, and whether Defendant breached that duty to provide timely notice;

j. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct was *per se* negligent;

m. Whether Defendant breached any contractual duties to provide adequate security for the Private Information entrusted to it, duties

that were either explicit or implied by the imposition of the "Technology Fee" of $470.

n. Whether Defendant was unjustly enriched;

o. Whether Defendant's conduct violated federal law;

p. Whether Defendant's conduct violated state law;

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

111. Common sources of evidence may also be used to demonstrate Defendant's unlawful conduct on a class-wide basis, including, but not limited to, documents and testimony about its data and cybersecurity measures (or lack thereof); testing and other methods that can prove Defendant's data and cybersecurity systems have been or remain inadequate; documents and testimony about the source, cause, and extent of the Data Breach; and documents and testimony about any remedial efforts undertaken as a result of the Data Breach.

112. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach and due to Defendant's misfeasance.

113. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel

experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

114. Predominance, Fed. R. Civ. P. 23 (b)(3). Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

115. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

116. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm

the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

117. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

118. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

119. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

120. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

121. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

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

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

g. Whether Defendant breached any contractual duty, either explicit or implied, to provide adequate data security as part of the "Technology Fee" of $470 assessed to each student of Defendant; and,

h. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

122. Defendant acted on grounds that apply generally to the Class as a whole, so that Class certification and the corresponding relief sought are appropriate on a Class-wide basis.

123. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

124. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

125. Plaintiff brings this claim individually and on behalf of the Class members.

126. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

127. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within their possession was compromised and precisely the type(s) of information that were compromised.

128. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

129. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority

like HIPAA and/or Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

130. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its Class Members, which is recognized by laws and regulations, as well as 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.

131. In addition, 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.

132. 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.

133. Defendant systematically failed to provide adequate security for data in its possession.

134. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Upon information and belief, mishandling emails, so as to allow for unauthorized person(s) to access Plaintiff's and Class Members' Private Information;

b. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

c. Failing to adequately monitor the security of their networks and systems;

d. Failure to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards.

135. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

136. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

137. Defendant, through its actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

138. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff and Class Members' Private Information would result in injury to Plaintiff and Class Members.

139. It was foreseeable that the failure to adequately safeguard Plaintiff and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

140. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

141. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members regarding what type of Private Information has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

142. Defendant's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

143. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

144. Plaintiff seeks the award of actual damages on behalf of the Class. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling Defendant to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

SECOND COUNT
Negligence *per se*
(On Behalf of Plaintiff and the Nationwide Class)

145. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

146. 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 Plaintiff and Class Members' Private Information.

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

148. 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 their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

149. The harm that occurred as a result of the Data Breach is the type of harm that the Federal Trade Commission Act was intended to guard against.

150. Defendant breached their duties to Plaintiff and Class Members under the Federal Trade Commission Act, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

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

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

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

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

THIRD COUNT
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

155. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

156. Defendant, as a condition of providing its services, required Plaintiff and Class Members to provide and entrust their Private Information.

157. By Plaintiff and Class Members providing their Private Information, and by Defendant accepting this Private Information, the parties mutually assented to implied contracts. These implied contracts included an implicit agreement and understanding that (1) Defendant would adequately safeguard Plaintiff's and Class Members' Private Information from foreseeable threats, (2) that Defendant would delete the information of Plaintiff and Class Members once it no longer had a legitimate need; and (3) that Defendant would provide Plaintiff and Class Members with notice within a reasonable amount of time after suffering a data breach.

158. Defendant provided consideration by providing it services, while Plaintiff and Class Members provided consideration by providing valuable property—i.e., their Private Information and payment of the Technology Campus Facility Fee. Defendant benefitted from the receipt of this Private Information by increased income.

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

160. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their Private Information, or providing timely and accurate notice to them that their Private Information was compromised due to the Data Breach.

161. Defendant' breaches of contract have caused Plaintiff and Class Members to suffer damages from the lost benefit of their bargain, out of pocket monetary losses and expenses, loss of time, and diminution of the value of their Private Information.

162. As a direct and proximate result of Defendant' above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

FOURTH COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class)

163. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

164. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information, as well as through payment of the Carnegie Mellon University Technology Fee.

165. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

166. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant' failure to provide the requisite security.

167. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

168. Defendant acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

169. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide it to Defendant.

170. Plaintiff and Class Members have no adequate remedy at law.

171. As a direct and proximate result of Defendant' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control or direct how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized

use of their Private Information; (v) 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; (vi) the continued risk to their Private Information, which remains in Defendant' possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

172. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

173. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

FIFTH COUNT
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Nationwide Class)

174. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

175. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

176. Defendant owed a duty of care to Plaintiff and Class Members that require it to adequately secure Plaintiff's and Class members' Private Information.

177. Defendant failed to fulfill their duty of care to safeguard Plaintiff's and Class Members' Private Information.

178. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class members are at risk of additional or further harm due to the exposure of their Private Information and Defendant' failure to address the security failings that led to such exposure.

179. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's contractual obligations and legal duties.

180. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage internal security personnel to conduct testing, including 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;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for their provision of services;

e. Ordering that Defendant conduct regular database scanning and security checks; and

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, Plaintiff and Class Members' Personally Identifiable Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for relief as follows:

A. For an Order certifying this case as a class action and appointing Plaintiff and Plaintiff's 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 Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to

disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

F. Ordering Defendant to disseminate individualized notice of the Data Breach to all Class Members;

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

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

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

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

Dated: April 3, 2025

By: *s/ Glen L. Abramson*

Glen L. Abramson (PA Bar No. 78522)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: (866) 252-0878
gabramson@milberg.com

Bryan L. Bleichner*
Philip Krzeski*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

**Pro Hac Vice Application forthcoming*

Counsel for Plaintiff and Putative Class Members