**UNITED STATES DISTRICT COURT**
**NORTHERN DISTRICT OF TEXAS**
**DALLAS DIVISION**

| | |
|---|---|
| IN RE VARSITY BRANDS, INC. DATA BREACH LITIGATION,<br><br>This Document Relates To: All Cases | Master File No. 3:24-cv-02633-B<br><br>JURY TRIAL DEMANDED |

# CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Dean Huntley, Tony Le, and Wanetta London ("Plaintiffs"), individually and on behalf of all others similarly situated, for their Consolidated Class Action Complaint, bring this action against Defendant Varsity Brands, Inc. ("Defendant" or "Varsity Brands")[1] based on personal knowledge and the investigation of counsel and alleges as follows:

## I. INTRODUCTION

1. Through this action, Plaintiffs seek to hold Defendant responsible for the harms it caused Plaintiffs and similarly situated persons in the preventable data breach of Defendant's inadequately protected computer network.

2. On May 24, 2024, Varsity Brands detected suspicious activity on its computer network, indicating a data breach by an unauthorized third-party. Based on a subsequent forensic investigation, Varsity Brands determined that cybercriminals infiltrated its inadequately secured computer environment and thereby gained unauthorized access to its data files (the "Data

[1] "Defendant" or "Varsity Brands" specifically includes any and all of Varsity Brands' subsidiary entities.

Breach"). The investigation further determined by this infiltration cybercriminals potentially accessed and acquired files containing the sensitive Private Information of 65,669 individuals.[2]

3. The personally identifiable information ("PII") accessed by cybercriminals included names, dates of birth, Social Security numbers, financial account information, credit card information, and Driver's license numbers as well as private health information ("PHI") such as health insurance information (collectively with PII, "Private Information").[3]

4. Varsity Brands, the parent company of BSN Sports and Varsity Sports, is the leading provider of cheerleading, dance, and performing arts competitions, apparel, uniforms, footwear, training camps, and yearbooks. Varsity Brands has annual revenue of approximately $2.5 billion.[4]

5. In carrying out its business, Defendant obtains, collects, uses, and derives a benefit from the Private Information of Plaintiffs and the Class. As such, Defendant assumed the legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

6. Due to Defendant's negligence, cybercriminals obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

---

[2] Varsity Brands' breach notification letter, accessible at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/09043096-cc0d-444c-9dc0-76df8ddd3734.html; *see also* Exhibit 1 hereto.

[3] *See* https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (identifying the information exposed in the Data Breach).

[4] https://www.dallasnews.com/business/retail/2023/09/06/varsity-brands-sells-its-herff-jones-high-school-college-graduation-business/.

7. This class action seeks to redress Defendant's negligence, unlawful, willful and wanton failure to protect the personal identifiable information of possibly thousands of individuals that was exposed in a major data breach of Defendant's network in violation of its legal obligations.

8. Defendant's negligence and misconduct – failing to implement adequate and reasonable measures to protect Plaintiff's and Class members' Private Information, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that it did not have adequate security practices in place to safeguard the Private Information, and failing to provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiff and Class members across the United States.

9. For the rest of their lives, Plaintiffs and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Plaintiffs and Class Members will have to spend time responding to the Breach and are at an immediate, imminent, and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred and/or will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their PII, loss of privacy, and/or additional damages as described below.

10. Defendant betrayed the trust of Plaintiffs and the other Class Members by failing to properly safeguard and protect their Private Information and thereby enabling cybercriminals to steal such valuable and sensitive information.

11. Plaintiffs bring this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs,

injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

## II. THE PARTIES

12. Plaintiff Dean Huntley is a resident of Indiana. Plaintiff Huntley received a Notice of Data Breach letter from Varsity Brands dated October 14, 2024, informing him that his Private Information was obtained in the Data Breach.

13. Plaintiff Tony Le is a resident of Texas. Plaintiff Le received a Notice of Data Breach letter from Varsity Brands dated October 14, 2024, informing him that his Private Information was obtained in the Data Breach.

14. Plaintiff Wanetta London is a resident of Indiana. Plaintiff London received a Notice of Data Breach letter from Varsity Brands dated October 14, 2024, informing her that her Private Information was obtained in the Data Breach.

15. Defendant Varsity Brands is incorporated in Delaware with its headquarters located in Framers Branch, Texas.

16. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

## III. JURISDICTION AND VENUE

17. This Court has subject matter and diversity 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 million, exclusive of interest and costs; there are more than 100 members in the proposed class; and at least one Class Member, including a named Plaintiffs, is a citizen of a state different from Defendants to establish minimal diversity.

18. Defendant is a citizen of Texas because it is incorporated in Texas with its headquarters in this District.

19. This Court has personal jurisdiction over Defendant because it conducts substantial business in Texas and this District and collected and/or stored the Private Information of Plaintiffs and Class Members in this District.

20. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiffs and the Class Members' claims occurred in this District, including Defendant collecting and/or storing the Private Information of Plaintiffs and Class Members.

## IV. FACTUAL ALLEGATIONS

***Background***

21. Varsity Brands is an apparel company focused on academic apparel and school memorabilia.

22. Defendant employs approximately 9,000 people across the United States.

23. Plaintiffs and Class Members are current and former employees of Varsity Brands or its affiliates.

24. In order to gain employment with Defendant, Defendant requires Plaintiffs' and Class Members' PII, including their names, dates of birth, email addresses, physical addresses, Social Security numbers, health insurance information, financial information, and Driver's license numbers.

25. Defendant collected, stored, and maintained the Private Information of Plaintiffs and the Class Members on its network. Defendant, however, failed to take reasonable and necessary steps to ensure that its network was secure.

26. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

27. Under state and federal law, businesses like Defendant have duties to protect its current and former employees' Private Information and to notify them about breaches.

28. Plaintiffs and the Class Members did not have control over how Defendant stored and maintained their Private Information. Rather, Plaintiffs were at Defendant's mercy, as Defendant had sole control and authority over its protection of Plaintiffs' and the Class Members' Private Information.

29. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

30. Plaintiffs and other Members of the Class entrusted their Private Information to Defendant.

31. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use for information for business purposes only, and to only make authorized disclosures of this information. Plaintiffs and Class Members demanded security to safeguard their Private Information.

32. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and the Class Members from involuntary disclosure to third parties.

33. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect its consumers' Private

Information or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. Rather, Defendant chose to store Plaintiffs' and the Class Members' Private Information on an unsecure network, leaving their Private Information vulnerable for cybercriminals to take. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to employees' Private Information.

***The Data Breach***

34. On or around May 14, 2024, Varsity Brands identified suspicious activity on its network. Based on a subsequent investigation, forensic investigators concluded that, due to Defendant's failure to maintain an adequate security system, unknown hackers infiltrated Defendant's network and "obtained" certain files and information from Defendant's systems. The information accessed and copied by cybercriminals includes Plaintiffs and Class Members' Private Information, including (but not limited to) their names, dates of birth, Social Security numbers, financial account information, and employee IDs.[5]

35. Despite the sensitivity of the Private Information that was exposed and the known attendant consequences to the affected individuals, Defendant was further negligent and failed to disclose the Data Breach for several months. Indeed, Varsity Brands did not begin sending breach notification letters to affected individuals until October 14, 2024—***five months*** after Varsity Brands discovered the Data Breach. This inexplicable delay further exacerbated the harms to Plaintiffs and the Class Members.

[5] *See* https://sgbonline.com/bsn-sports-parent-hit-by-data-breach/; https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage.

36. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of employees like Plaintiffs and Class Members.

37. Upon information and belief, the unauthorized third-party cybercriminal gained access to the Private Information, exfiltrated the Private Information from Defendant's network, and has engaged in (and will continue to engage in) misuse of the Private Information, including marketing and selling Plaintiffs' and the Class Members' Private Information on the dark web. Indeed, counsel's investigation reveals that cybercriminals have posted the Private Information of Varsity Brands' employees, including Plaintiff Huntley, for sale on the dark web following the Data Breach. Many of the dark web posts specifically attribute the source of the Private Information as coming from Varsity Brands.

38. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected. Nor has Defendant disclosed what, if anything, it has done to improve its cyber security to prevent a repeat of its negligence and failure to protect Class Members Private Information.

39. Given the type of targeted attack in this case, the type of Private Information accessed, and the fact that such information was successfully exfiltrated by cybercriminals, there is a strong probability that the unencrypted Private Information of Plaintiffs and Class Members have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes. In fact, Plaintiff Huntley's Private Information has already been posted on the dark web since the Data Breach.

40. Defendant was negligent and did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of Private Information for Plaintiffs and Class Members.

41. For example, as evidenced by the Data Breach's occurrence, the infiltrated network was not protected by sufficient multi-layer data security technologies or effective firewalls.

42. Similarly, based on the delayed discovery of the Data Breach, it is evident that the infiltrated network, that Defendant allowed to store Plaintiffs' Private Information, did not have sufficiently effective endpoint detection.

43. Further, the fact that PII was acquired in the Data Breach demonstrates that the PII contained in the Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

44. Plaintiffs and Class Members entrusted Defendant with sensitive and confidential information, including their PII, which includes information (such as Social Security numbers) that are static, do not change, and can be used to commit a myriad of financial crimes.

45. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

46. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

47. Because Defendant had a duty to protect Plaintiffs' and Class Members' Private Information, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

48. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. 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 and cyber-attacks;

b. Failing to adequately protect its employees' Private Information;

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

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic Private Information it created, received, maintained, and/or transmitted;

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic Private Information to allow access only to those persons or software programs that have been granted access rights;

h. Failing to implement policies and procedures to prevent, detect, contain, and

correct security violations;

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic Private Information;

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PII that are not permitted under the privacy rules;

l. Failing to train all members of its workforces effectively on the policies and procedures regarding PII as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of Private Information;

m. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic Private Information;

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

o. Failing to adhere to industry standards for cybersecurity; and

p. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

49. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted Private Information.

50. Accordingly, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant.

***The Data Breach was Foreseeable Risk of Which Defendant was on Notice***

51. Because Defendant had a duty to protect Plaintiffs' and Class Members' Private Information, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

52. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

53. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[6]

54. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.[7]

55. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize

[6] *See* 2021 Data Breach Annual Report, ITRC 6 (Jan. 2022), available at https://www.idtheftcenter.org/notified (last visited Dec. 7, 2023).
[7] *2022 End of Year Data Breach Report*, Identity Theft Resource Center (Jan. 25, 2023), available at: https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report.

damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[8]

56. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[9]

57. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that: (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of companies in possession of significant sensitive information such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

58. Considering the information readily available and accessible on the internet before the Data Breach and Defendant's involvement in data breach litigation, Defendant, having elected to store the unencrypted Private Information of Plaintiffs and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the Private Information, and Defendant's type of business had cause to be particularly on guard against such an attack.

---

[8] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), available at https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Jan. 25, 2022).

[9] U.S. CISA, Ransomware Guide – September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited Jan. 25, 2022).

59. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' Private Information could be accessed, exfiltrated, and published as the result of a cyberattack.

60. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted or destroyed the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

***The Data Breach was Preventable***

61. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

62. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[10]

63. To prevent and detect ransomware attacks, including the ransomware attack 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 ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

[10] 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 July 17, 2023).

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[11]

64. To prevent and detect ransomware attacks, including the ransomware 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:

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

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

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

- **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 Private 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. . . .[12]

[12] *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 July 17, 2023).

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

**Secure internet-facing assets**
- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; Remove privilege credentials

**Thoroughly investigate and remediate alerts**
- Prioritize and treat commodity malware infections as potential full comprise

**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].[13]

66. Given that Defendant was storing the Private Information of other individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

[13] *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 July 17, 2023).

67. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiffs and Class Members.

68. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the Private Information of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

69. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

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

71. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Plaintiffs' and Class Members' Private Information was compromised through disclosure to an unknown and unauthorized criminal third party.

72. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable

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

73. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long-lasting and severe. Once Private Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

***Varsity Brands' History of Poor Oversight***

74. Varsity Brands has a history of implementing aggressive strategies while simultaneously maintaining insufficient oversight.

75. Indeed, multiple antitrust lawsuits have been filed against Varsity Brands, accusing Defendant of deploying monopolistic and collusive strategies to maintain its dominant position in the cheerleading events, gyms, and apparel industry. These lawsuits resulted in massive settlements, including recent settlements of $43.5 million in 2023 and $82.5 million in 2024.[14]

[14] *See Fusion Elite All Stars, et al. v. Varsity Brands, LLC, et al*., Case No. 2:20-cv-02600-SHL (W.D. Tenn.); *Jones, et al. v. Varsity Brands, LLC, et al.,* Case No. 2:20-cv-02892 (W.D. Tenn.).

76. While Defendant was aggressively fighting to increase its revenues within the cheerleading space, it was failing to protect the young participants who funded those revenues. Indeed, multiple lawsuits have been filed against Varsity Brands on allegations that Varsity Brands failed to protect the minors who participated in its cheerleading camps and competitions.[15]

***Defendant Failed to Adhere to FTC Guidelines***

77. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Private Information.

78. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[16] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[17]

79. In 2016, the FTC updated its publication, Protecting Private Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. Protect the sensitive consumer information that they keep;

---

[15] *See, e.g.,* https://www.sportico.com/law/news/2023/cheerleading-sex-abuse-lawsuit-varsity-bain-capital-1234726822/ (discussing lawsuits).

[16] 17 C.F.R. § 248.201 (2013).

[17] *Id.*

b. Properly dispose of PII that is no longer needed;

c. Encrypt information stored on computer networks;

d. Understand their network's vulnerabilities; and

e. Implement policies to correct security problems.

80. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

81. The FTC recommends that companies not maintain 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.

82. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("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.

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

***Defendant Fails to Comply with Industry Standards***

84. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the

Private Information which they collect and maintain.

85. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to; 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.

86. Other best cybersecurity practices that are standard in the healthcare industry 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.

87. Defendant failed to meet the minimum standards of any of the following frameworks: NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

88. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

89. Indeed, it was not until *after* the Data Breach was discovered that Varsity Brands hired its first Chief Security Officer. Specifically, while the Data Breach was discovered in May 2024, Defendant did not have a Chief Security Officer until June 26, 2024.[18]

***Defendant's Response to the Data Breach is Inadequate***

90. Defendant was negligent and failed to inform Plaintiffs and the Class Members of the Data Breach in time for them to protect themselves from identity theft.

91. Defendant admitted that it learned of the data breach as early as May 24, 2024. Yet, Defendant did not start notifying affected individuals until months later on or around October 2024. This is an inexcusable delay.

92. During these intervals, the cybercriminals have had the opportunity to exploit the Plaintiffs' and the Class Member's Private Information while Defendant was secretly investigating the Data Breach.

93. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

***Value of Private Information***

94. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, Private Information can be sold at a price

[18] https://www.varsitybrands.com/news/varsity-brands-appoints-chief-security-officer-and-invests-in-additional-safety-security-efforts-initiatives/.

ranging from $40 to $200, and bank details have a price range of $50 to $200.[19] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[20] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[21]

95. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

96. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[22]

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

98. One such example of criminals using Private Information for profit is the development of "Fullz" packages.

---

[19] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 17, 2023).

[20] *Here's How Much Your Private Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July17, 2023).

[21] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 17, 2023).

[22] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed July 17, 2023).

99. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

100. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

101. That is exactly what is happening to Plaintiffs and members of the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

***Plaintiffs' Injuries and Experiences***

***A. Plaintiff Huntley's Injuries and Experiences***

102. Plaintiff Huntley is a former employee of BSN Sports, a subsidiary of Varsity Brands. Plaintiff Huntley entrusted his Private Information to Defendant in exchange for employment opportunities.

103. Plaintiff and Class members' Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

104. Plaintiff Huntley received a notice letter from Defendant dated October 14, 2024, informing him that his Private Information—including his Social Security number—was specifically identified as having been exposed to an unauthorized third party in the Data Breach.

105. Plaintiff Huntley is very careful about sharing his sensitive information. To the best of Plaintiff Huntley's knowledge, he has never before had his Private Information exposed in any other data breach.

106. Plaintiff Huntley stores any documents containing his Private Information in a safe and secure location. Plaintiff Huntley has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

107. Because of the Data Breach, Plaintiff Huntley's Private Information is now in the hands of cybercriminals.

108. Plaintiff Huntley has suffered actual injury from the exposure and theft of his Private Information, which violates his right to privacy.

109. As a result of the Data Breach, which exposed highly valuable Private Information, Plaintiff Huntley is now imminently at risk of crippling future identity theft and fraud.

110. Since the Data Breach, Plaintiff Huntley has experienced identity theft in the form of fraudulent financial charges that took place in the summer of 2024. In addition, since the Data Breach Plaintiff Huntley has experienced a notable increase in spam call, including calls in which people are impersonate Medicare representatives. On these calls, they are able to recite some of Plaintiff Huntley's Private Information to him. Plaintiff Huntley attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, and the fact that he has never experienced anything like this prior to now.

111. Moreover, Plaintiff Huntley's information has been located on the dark web following the Data Breach. Indeed, Plaintiff Huntley's Private Information (including files purporting to include his Social Security number and direct deposit information) has been posted for sale on various sites since May 2024.

112. As a result of the Data Breach, Plaintiff Huntley has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Huntley has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach. In particular, Plaintiff Huntley has expended time to research facts about the Data Breach, thoroughly review account statements, monitor his account activity and other information, dispute the unauthorized financial transactions, address the increase in spam calls, and take other protective and ameliorative steps in response to the Data Breach.

113. The letter Plaintiff Huntley received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised that they should "vigilant against potential threats of identity theft or fraud by regularly monitoring your account statements and credit history for any signs of unauthorized activity."[23] In addition, the breach notification letter included a list of steps for Class Members to take to help protect themselves, including enrolling in credit monitoring, reviewing credit reports, and placing security freezes on credit reports.[24]

[23] *See* sample breach notification letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/09043096-cc0d-444c-9dc0-76df8ddd3734.html.

[24] *Id.*

114. As a result of the Data Breach, Plaintiff Huntley has experienced stress and immense worry due to the loss of his privacy. Plaintiff Huntley is concerned over the impact of cybercriminals misusing his Private Information. Plaintiff Huntley fears that criminals will use his information to commit identity theft.

115. Plaintiff Huntley anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

116. Plaintiff Huntley has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff Huntley's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Huntley's Private Information being placed in the hands of an unauthorized third party; (c) damages to and/or diminution in value of Plaintiff Huntley's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff Huntley, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Huntley's Private Information; and (e) continued risk to Plaintiff Huntley's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

***B. Plaintiff Le's Injuries and Experience***

117. Plaintiff Le entrusted his Private Information to Varsity Brands in exchange for employment opportunities. Plaintiff and Class members' Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

118. Plaintiff Le received a notice letter from Defendant dated October 14, 2024, informing him that his Private Information—including his Social Security number—was specifically identified as having been exposed to an unauthorized third party in the Data Breach.

119. Plaintiff Le is very careful about sharing his sensitive information. To the best of Plaintiff's knowledge, he has never before had his Private Information exposed in any other data breach.

120. Plaintiff Le has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

121. Because of the Data Breach, Plaintiff Le's Private Information is now in the hands of cybercriminals.

122. Plaintiff Le has suffered actual injury from the exposure and theft of his Private Information, which violates his right to privacy.

123. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Le is now imminently at risk of crippling future identity theft and fraud.

124. Since the Data Breach, Plaintiff Le has experienced a noticeable increase in spam emails. Plaintiff Le attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, and the fact that the recent influx of spam calls is unusual.

125. As a result of the Data Breach, Plaintiff Le has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Le has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data

Breach, researching and enrolling in credit monitoring, thoroughly reviewing account statements and credit reports, and taking other protective and ameliorative steps in response to the Data Breach.

126. The letter Plaintiff Le received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised the to "remain vigilant against potential threats of identity theft or fraud by regularly monitoring your account statements and credit history for any signs of unauthorized activity."[25] In addition, the breach notification letter included steps for Class Members to take to help protect themselves from the impact of the Data Breach including, enrolling in credit monitoring, reviewing credit reports, and placing security freezes on credit reports.[26]

127. As a result of the Data Breach, Plaintiff Le has experienced stress, anxiety, and frustration due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Le fears that criminals will use his information to commit identity theft.

128. Plaintiff Le anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

129. Plaintiff Le has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Le's Private Information being placed in the hands of an unauthorized third party; (c) damages to and/or diminution in value of Plaintiff Le's Private Information that was entrusted to Defendant; (d)

[25] *Id.*
[26] *Id.*

damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Le's Private Information; and (e) continued risk to Plaintiff Le's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

### *C. Plaintiff London's Injuries and Experience*

130. Plaintiff London entrusted her Private Information to Varsity Brands in exchange for employment opportunities.

131. Plaintiff and Class members' Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

132. Plaintiff London received a notice letter from Defendant dated October 14, 2024, informing her that her Private Information—including her Social Security number—was specifically identified as having been exposed to an unauthorized third party in the Data Breach.

133. Plaintiff London is very careful about sharing her sensitive information. To the best of Plaintiff's knowledge, she has never before had her Private Information exposed in any other data breach.

134. Plaintiff London stores any documents containing her Private Information in a safe and secure location. Plaintiff London has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

135. Because of the Data Breach, Plaintiff London's Private Information is now in the hands of cybercriminals.

136. Plaintiff London has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

137. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff London is now imminently at risk of crippling future identity theft and fraud.

138. As a result of the Data Breach, Plaintiff London has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff London has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, and thoroughly reviewing account statements and credit statements.

139. The letter Plaintiff London received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised them to "remain vigilant against potential threats of identity theft or fraud by regularly monitoring your account statements and credit history for any signs of unauthorized activity."[27] In addition, the breach notification letter included steps for Class Members to take to help protect themselves including, enrolling in credit monitoring, reviewing credit reports, and placing security freezes on credit reports.[28]

[27] *Id.*
[28] *Id.*

140. As a result of the Data Breach, Plaintiff London fears that criminals will use her information to commit identity theft.

141. Plaintiff London anticipates continuing to spend considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

142. Plaintiff London has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff London's Private Information being placed in the hands of an unauthorized third party; (c) damages to and/or diminution in value of Plaintiff London's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff London's Private Information; and (e) continued risk to Plaintiff London's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant

***Plaintiffs and the Class Face Significant Risk of Continued Identity Theft***

143. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their Private Information that can be directly traced to Defendant.

144. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their Private Information that can be directly traced to Defendant.

145. Defendant negligently disclosed the Private Information of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up,

disclosed, and exposed the Private Information of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

146. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's database, amounting to potentially thousands of individuals' detailed, Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

148. The injuries to Plaintiffs and Class Members are directly and proximately caused by Defendant's negligence and failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

149. As a result of Defendant's negligence and failure to prevent the Data Breach, Plaintiffs and the Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. Identity theft;

b. Misuse of their Private Information;

c. The loss of the opportunity to control how their Private Information is used;

d. The diminution in value of their Private Information;

e. The compromise and continuing publication of their Private Information;

f. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

g. Loss opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spend researching how to prevent, detect, contest, and recover form identity theft and fraud;

h. Delay in receipt of tax refund monies;

i. Unauthorized use of stolen Private Information; and

j. The continued risk to their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Private Information in their possession.

***Plaintiffs' and the Class Members' Private Information is Available on the Dark Web***

150. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' Private Information with the intent of engaging in misuse of the Private Information, including marketing and selling Plaintiffs' and Class Members' Private Information.

151. Upon information and believe, the unencrypted Private Information of Plaintiffs and Class Members is for sale on the dark web. Not only is this the *modus operandi* of hackers, but counsel's investigation discovered that Varsity Brands' employee information, including

Plaintiff Huntley's Private Information, is (and has been) posted for sale on the dark web.

152. Plaintiff Huntley has already experienced identity theft and fraud. Plaintiff did not have any issues with this prior to the Data Breach. As such, Plaintiff Huntley reasonably believe that his information, and the Class's information, was sold on the dark web, resulting in the fraudulent misuse.

153. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[29] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[30] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

154. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, Private Information like the Private Information at issue here.[31] The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social

[29] *What Is the dark web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[30] *Id.*

[31] *What is the dark web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

Security numbers, dates of birth, and medical information.[32] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[33]

***Plaintiffs and the Class Members Have Experienced Misuse***

155. As a result of the Data Breach, the unencrypted and detailed Private Information of Plaintiffs and the Class Members has fallen into the hands of companies that will use it for targeted marketing without the approval of Plaintiffs and Class Members, as seen by the increase in spam calls and emails. Unauthorized actors can easily access and misuse Plaintiffs' and Class Members' Private Information due to the Data Breach. Plaintiffs have already experienced misuse of their Private Information as a result of the Data Breach.

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

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

158. For example, armed with just a name and Social Security number, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information

[32] *Id.; What Is the dark web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[33] *What is the dark web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

about a victim's identity, such as a person's login credentials or financial account information. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or Private Information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

159. Moreover, the existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

160. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

161. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

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

> A dishonest person who has your Social Security number can use it to get other Private Information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[34]

[34] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

163. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

164. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[35]

165. 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 obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's Private Information to police during an arrest resulting in an arrest warrant issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for credit lines.[36]

166. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice,

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or Private Information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were

[35] 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 visited Aug. 23, 2024).

[36] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), available at https://www.ssa.gov/pubs/EN-05-10064.pdf.

> reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[37]

167. 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.[38]

168. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[39] Yet, Defendants failed to rapidly report to Plaintiffs and Class Members that their Private Information was stolen.

***Plaintiffs' and the Class Members' Lost Time***

169. Plaintiffs and the Class Members have also spent considerable time and will continue to spend considerable time to protect themselves and keep their identities and personal property protected.

170. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[40]

---

[37] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Jan. 23, 2024).

[38] https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

[39] *Id.*

[40] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=%20In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20 per%20hour (last accessed March 18, 2024); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data*, https://www.bls.gov/news.release/pdf/wkyeng.pdf (last accessed May 9 2024) (finding that on average, private-sector workers make $1,145 per 40-hour work week.).

171. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week; leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[41] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

172. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

***Plaintiffs' and the Class Members' Heightened Risk of Identity Theft and Ongoing Injuries***

173. Cyberattacks and data breaches at healthcare companies and partner companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

174. 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 face "substantial costs and time to repair the damage to their good name and credit record."[42]

175. 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

[41] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019) (last accessed May 9, 2024).

[42] *See* U.S. Gov't Accounting Office, GAO-07-737, Private 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 (last visited March 18, 2024).

information is to monetize it 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. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or Private Information through means such as spam phone calls and text messages or phishing emails.

176. 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 seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[43]

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

178. 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

[43] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited March 18, 2024).

and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's Private Information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

179. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[44]

180. 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.

181. Additional fraudulent activity resulting from the Data Breach may not come to light for years.

182. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[45]

---

[44] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[45] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed July 17, 2023).

183. As a result of the Data Breach, Cybercriminals also have sufficient information to pose as legitimate persons and gain more information from Plaintiffs and the Class Members, putting Plaintiffs and the Class Members at a continuing risk of identity theft.

184. 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.

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

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

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

188. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

***Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary***

189. To date, Defendant has offered Plaintiffs and some Class Members an inadequate amount of credit monitoring services. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly considering the nature of the Private Information at issue here.

190. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money, filing false tax returns, taking out loans or lines of credit, or filing false unemployment claims.

191. Such fraud may go undetected until debt collection calls commence months, or even years, later. 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.

192. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[46] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

[46] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The dark web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

193. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future, if not forever.

194. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

## V. CLASS ACTION ALLEGATIONS

195. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

196. The nationwide Class that Plaintiffs seek to represent is defined as follows:

> All United States residents who were sent a letter notifying them that their Private Information was actually or potentially accessed and/or acquired in the Data Breach (the "Class").

197. 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.

198. Plaintiffs reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

199. **Numerosity (Fed R. Civ. P. 23(a)(1)):** The Class is so numerous that joinder of all members is impracticable. Potentially thousands of individuals' information was subjected to this Data Breach.

200. **Commonality (Fed. R. Civ. P. 23(a)(2) & (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 and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. Whether Defendant failed to timely destroy the Private Information of Plaintiffs and the Class Members;

f. When Defendant actually learned of the Data Breach;

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

h. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

i. 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;

j. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

k. Whether Defendant engaged in unfair, unlawful, or deceptive practice by failing to safeguard the Private Information of Plaintiffs and Class Members;

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

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

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

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

202. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

203. **Adequacy (Fed. R. Civ. P. 23(a)(4)):** Plaintiffs will fairly and adequately represent and protect the interests of Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

204. **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.

205. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it 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 Plaintiffs were 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.

206. 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.

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

208. 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.

209. 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 Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to

exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, safeguarding, and failing to destroy 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 Plaintiffs 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 Plaintiffs and Class Members; and,

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

## VI. CAUSES OF ACTION

### COUNT I – NEGLIGENCE
**(On Behalf of Plaintiffs and the Class)**

211. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

212. Defendant solicited, gathered, and stored the Private Information Plaintiffs and the Class as part of the operation of its business.

213. Upon accepting and storing the Private Information of Plaintiffs and Class Members, Defendant undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

214. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiffs and Class members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

215. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their Private Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

216. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive Private Information.

217. Defendant owed Plaintiffs and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing Private Information, including taking action to reasonably safeguard such data.

218. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard Private Information.

219. Defendant had duties to protect and safeguard the Private Information of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiffs and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class Members' Private Information was adequately secured from impermissible access, viewing, release, disclosure, and publication;

b. To protect Plaintiffs' and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving their networks and servers; and

d. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

220. Defendant was the only one who could ensure that its systems and protocols were sufficient to protect the Private Information that Plaintiffs and the Class had entrusted to it.

221. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties the FTC Act. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy and

significant risk of identity theft, are the types of harm that these statutes and their regulations were intended to prevent.

222. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

223. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders also form part of the basis of Defendant's duty in this regard.

224. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect consumers PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and Class Members.

225. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendant's violation of the FTC Act establishes the duty and breach elements of negligence.

226. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

227. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act 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 Plaintiffs and the Class.

228. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately train its employees to not store Private Information longer than absolutely necessary;

d. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's Private Information; and

e. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions.

229. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

230. As a proximate and foreseeable result of Defendant's negligent and/or grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages.

231. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiffs and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiffs and Class Members while it was within Defendant's possession and control.

232. As a result of the Data Breach, Plaintiffs and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies and the payment for credit monitoring and identity theft prevention services.

233. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

234. The damages Plaintiffs and the Class have suffered and will suffer were and are the direct and proximate result of Defendant's negligent and/or grossly negligent conduct.

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

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

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

## COUNT II – BREACH OF IMPLIED CONTRACT
**(On Behalf of Plaintiffs and the Class)**

238. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

239. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of receiving employment provided by Defendant.

240. Plaintiffs and Class Members entrusted their PII to Defendant. In doing so, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their Private Information and to timely notify them in the event of a Data Breach.

241. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PII to Defendant with the reasonable understanding that their PII would be adequately protected from foreseeable threats. This inherent understanding exists independent of any other law or contractual obligation any time that highly sensitive PII is exchanged as a condition of receiving services. It is common sense that but for this implicit and/or explicit agreement, Plaintiffs and Class Members would not have provided their PII to Defendant.

242. Based on Defendant's conduct, representations, legal obligations, and acceptance of Plaintiffs' and the Class Members' Private Information, Defendant had an implied duty to safeguard their Private Information through the use of reasonable industry standards. This implied duty was reinforced by Defendant's representations in its Privacy Policy, which provides, *inter alia*:

> We have implemented administrative, technical, and physical security measures to protect against the loss, misuse and/or alteration of your information. These safeguards vary based on the sensitivity of the information that we collect and store.[47]

243. Plaintiffs and the Class Members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for employment.

[47] *See* Varsity Brands' Privacy Policy available at: https://www.varsitybrands.com/privacy-policy/#security.

244. In turn, and through internal policies, Defendant agreed to protect and not disclose the Private Information to unauthorized persons.

245. Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's Private Information.

246. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class members with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

247. After all, Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of such an agreement with Defendant.

248. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

249. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain.

250. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

251. Defendant materially breached the contracts it entered with Plaintiffs and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

252. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiffs' and the Class Members' Private Information.

**COUNT III – UNJUST ENRICHMENT**
**(On Behalf of Plaintiffs and the Class)**

253. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

254. Plaintiffs and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from using their employment and Private Information to derive profit and facilitate its business.

255. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class Members.

256. Plaintiffs and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

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

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

259. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class Members' employment and Private Information because Defendant failed to adequately protect their Private Information.

260. Plaintiffs and Class Members have no adequate remedy at law.

261. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

## COUNT VI – DECLARTORY JUDGMENT
**(On Behalf of Plaintiffs and the Class)**

262. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

263. 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. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

264. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Class's Private Information and whether Defendant is currently maintaining data

security measures adequate to protect Plaintiffs and the Class from further data breaches that compromise their Private Information. Plaintiffs alleges that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs continues to suffer injury as a result of the compromise of her Private Information and remains at imminent risk that further compromises of their Private Information will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

265. Plaintiffs and the Class have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiffs' and the Class's Private Information, including Social Security numbers, while storing it in an Internet-accessible environment, and (ii) Defendant's failure to delete Private Information it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security numbers of Plaintiffs and the Class.

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

a. Defendant owes a legal duty to secure the Private Information of Plaintiffs and the Class;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs and the Class harm.

267. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' Private Information. Specifically, this injunction should,

among other things, direct Defendant to:

a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards;

d. implement an education and training program for appropriate employees regarding cybersecurity.

268. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

269. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

270. 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 at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and others whose

confidential information would be further compromised.

## VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

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

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

iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

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

v. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner employee data not necessary for their provisions of services;

vi. Ordering that Defendant conduct regular database scanning and securing checks; and

vii. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

## VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Dated: January 3, 2025

Respectfully submitted,

*/s/ William B. Federman*
William B. Federman
Jessica A. Wilkes
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 235-1560
-and-
212 W. Spring Valley Road
Richardson, TX 75081
wbf@federmanlaw.com
jaw@federmanlaw.com

A. Brooke Murphy
**MURPHY LAW FIRM**
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
T: (405) 389-4989
E: abm@murphylegalfirm.com

*Interim Class Counsel on behalf of Plaintiffs*

Joe Kendall
Texas Bar No. 11260700
**KENDALL LAW GROUP, PLLC**
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Telephone: 214/744-3000
Fax: 214/744-3015
jkendall@kendalllawgroup.com

*Interim Liaison Counsel*

# ClassAction.org