UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
TACOMA DIVISION

SHAYNA MARIE LANDIN, on behalf of herself individually and on behalf of all others similarly situated, Plaintiff, v. HI-SCHOOL PHARMACY SERVICES, LLC, and HI-SCHOOL PHARMACY, INC. Defendants.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR A JURY TRIAL**

Plaintiff Shayna Marie Landin ("Plaintiff") bring this Class Action Complaint ("Complaint") against Defendant Hi-School Pharmacy Services, LLC and Hi-School Pharmacy, Inc. ("Hi-School" or "Defendant")[1] as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

[1] On information and belief, Hi-School Pharmacy, Inc. and Hi-School Pharmacy, LLC operate together and do business as "Hi-School Pharmacy." Throughout this Complaint, Hi-School Pharmacy, Inc. and Hi-School Pharmacy, LLC will collectively be referred to as "Hi-School" unless otherwise noted.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

INTRODUCTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") that was perpetuated against Hi-School, "an independently owned and operated company[]" that provides pharmaceutical products and/or services to its customers.[2]

2. Plaintiff's and Class Members' sensitive personal information—which they entrusted to Hi-School—was compromised and unlawfully accessed due to the Data Breach.

3. Hi-School collected and maintained certain personally identifiable information of Plaintiff and the putative Class Members (defined below), who are (or were) employees at Hi-School.

4. The PII compromised in the Data Breach included Plaintiff's and Class Members' names, dates of birth, and Social Security numbers ("personally identifying information" or "PII").

5. The PII compromised in the Data Breach was targeted and exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals.

6. As a result of the Data Breach, Plaintiff and approximately 17,000 Class Members,[3] suffered concrete injury in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual

[2] https://myhspstores.com/our-company/

[3] According to the breach report submitted to the Office of the Maine Attorney General, 17,676 persons were impacted in the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/47edbdd7-acf2-428a-9440-4f1ffccce7a0.shtml

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Hi-School's possession and is subject to further unauthorized disclosures so long as Hi-School fails to undertake appropriate and adequate measures to protect the PII.

7. The Data Breach was a direct result of Hi-School's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its employees' PII from a foreseeable and preventable cyber-attack.

8. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Hi-School's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

9. Hi-School maintained the PII in a reckless manner. In particular, the PII was maintained on Hi-School's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Hi-School, and thus, Hi-School was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

10. Hi-School disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' PII; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

11. Plaintiff's and Class Members' identities are now at risk because of Hi-School's negligent conduct because the PII that Hi-School collected and maintained is now in the hands of data thieves.

12. Armed with the PII accessed in the Data Breach, data thieves have already engaged in identity theft and fraud, and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

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

14. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

15. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

16. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief, including improvements to Hi-School's data security systems, future annual audits, and adequate credit monitoring services funded by Hi-School.

17. Accordingly, Plaintiff brings this action against Hi-School seeking redress for its unlawful conduct.

PARTIES

18. Plaintiff Shayna Marie Landin is and has been at all relevant times a resident and citizen of Molalla, Oregon. Plaintiff received a Notice Letter, directly from Hi-School, via U.S. mail, dated December 5, 2023 (the "Notice Letter"). If Ms. Landin had known that Hi-School would not adequately protect her PII, she would not have entrusted Hi-School or anyone in Hi-School's position with her PII or allowed Hi-School to maintain this sensitive PII.

19. Hi-School Pharmacy Services, LLC is limited liability company organized under the state laws of Washington with its principal place of business located in Vancouver, Washington. Hi-School Pharmacy Services, LLC is owned by Hi-School Pharmacy, Inc., a Washington corporation with its principal place of business located in Vancouver, Washington.

20. Hi-School Pharmacy, Inc. is a Washington corporation with its principal place of business in Vancouver, Washington.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members, including Plaintiff, are citizens of

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

a different state than Hi-School. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

22. This Court has personal jurisdiction over Hi-School because it operates and maintains its principal place of business in this District and the computer systems implicated in this Data Breach are likely based in this District. Further, Hi-School is authorized to and regularly conducts business in this District and makes decisions regarding corporate governance and management of its businesses in this District, including decisions regarding the security measures to protect its employees' PII.

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

FACTUAL ALLEGATIONS

Hi-School's Business

24. Hi-School is "an independently owned and operated company" that provides pharmaceutical products and/or services to its customers.[4]

25. Plaintiff and Class Members are current or former employees at Hi-School.

26. As a condition of obtaining employment and/or obtaining certain employee benefits at Hi-School, Hi-School requires that its employees, including Plaintiff and Class Members, entrust it with highly sensitive personal information.

[4] https://myhspstores.com/our-company/

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

27. The information held by Hi-School in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

28. Upon information and belief, Hi-School made promises and representations to its employees, including Plaintiff and Class Members, that the PII collected from them as a condition of their employment and/or receiving benefits at Hi-School would be kept safe, confidential, that the privacy of that information would be maintained, and that Hi-School would delete any sensitive information after it was no longer required to maintain it.

29. Indeed, Hi-School's Privacy Policy provides that: "[w]e take reasonable measures to protect the information we collect from unauthorized access, disclosure, or use."[5]

30. Plaintiff and Class Members provided their PII to Hi-School with the reasonable expectation and on the mutual understanding that Hi-School would comply with its obligations to keep such information confidential and secure from unauthorized access.

31. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Hi-School to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

32. Hi-School had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Hi-School has a legal duty to keep employees' PII safe and confidential.

[5] https://myhspstores.com/privacy-policy/

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

33. Hi-School had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

34. Hi-School derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Hi-School could not perform the services it provides.

35. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Hi-School assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

The Data Breach

36. On or about December 5, 2023, Hi-School, began sending Plaintiff and other Data Breach victims a Notice of Data Security Incident letter (the "Notice Letter"), informing them that:

> **What Happened?** On November 3, 2023, Hi-School Pharmacy experienced a disruption in our computer network. We immediately initiated an investigation and engaged digital forensic experts to assist us with the process. The forensic investigation determined that certain personal information may have been acquired without authorization during the incident. We conducted a thorough review of the affected information and on November 21, 2023 determined that your information was involved. We then engaged a consumer remediation firm and worked with them to provide you notification and identity protection services as soon as possible.
>
> **What Information Was Involved?** The information may have included your name, date of birth, and/or Social Security number.[6]

37. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a

[6] The "Notice Letter." A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/47edbdd7-acf2-428a-9440-4f1ffccce7a0.shtml

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

38. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

39. Hi-School did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

40. The attacker accessed and acquired files Hi-School shared with a third party containing unencrypted PII of Plaintiff and Class Members, including their Social Security numbers and other sensitive information. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

41. Plaintiff believes that her PII and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

42. Hi-School did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

43. 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."[7]

44. To prevent and detect cyber-attacks and/or ransomware attacks Hi-School could and should have implemented, as recommended by the United States Government, the following measures:

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

[7] 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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

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.[8]

45. To prevent and detect cyber-attacks or ransomware attacks Hi-School could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

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

Thoroughly investigate and remediate alerts

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

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

[8] *Id.* at 3–4.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

- 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].[9]

46. Given that Hi-School was storing the PII of its current and former employees, Hi-School could and should have implemented all of the above measures to prevent and detect cyberattacks.

47. The occurrence of the Data Breach indicates that Hi-School failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of more than seventeen thousand current and former employees, including Plaintiff and Class Members.

Hi-School Acquires, Collects & Stores Employees' PII

48. Hi-School acquires, collects, and stores a massive amount of PII on its employees, former employees, and other personnel.

49. As a condition of employment, or as a condition of receiving certain benefits, Hi-School requires that employees, former employees, and other personnel entrust it with highly sensitive personal information.

[9] *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/

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

50. By obtaining, collecting, and using Plaintiff's and Class Members' PII, Hi-School assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

51. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

52. Plaintiff and the Class Members relied on Hi-School to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

53. Hi-School could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

54. Upon information and belief, Hi-School made promises to Plaintiff and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

55. Indeed, Hi-School's Privacy Policy provides that: "[w]e take reasonable measures to protect the information we collect from unauthorized access, disclosure, or use."[10]

56. Hi-School's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Hi-School Knew or Should Have Known of the Risk of the Risk Because Employers in Possession of PII are Particularly Suspectable to Cyber Attacks

57. Data breaches, including those perpetrated against employers that store PII in their systems, have become widespread.

[10] https://myhspstores.com/privacy-policy/

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

58. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[11]

59. Hi-School knew and understood unprotected or exposed PII in the custody of employers, like Hi-School, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

60. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Hi-School knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

61. Indeed, cyber-attacks, such as the one experienced by Hi-School, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[12]

---

[11] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/

[12] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

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

63. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

64. In the Notice Letter, Hi-School makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

65. Hi-School's offer of credit and identity monitoring establishes that Plaintiff's and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Hi-School's computer systems.

66. The injuries to Plaintiff and Class Members were directly and proximately caused by Hi-School's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

67. The ramifications of Hi-School's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

68. As a business in custody of current and former employees' PII, Hi-School knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Hi-School failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifiable Information

69. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[13] 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."[14]

70. The PII 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.[15]

[13] 17 C.F.R. § 248.201 (2013).

[14] *Id.*

[15] *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/

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

71. For example, Personal Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[16]

72. Criminals can also purchase access to entire company data breaches from $900 to $4,500.[17]

73. Social Security numbers, which were compromised for some of the Class Members as alleged herein, for example, are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[18]

74. 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.

---

[16] *Here's How Much Your Personal 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/

[17] *In the Dark*, VPNOverview, 2019, *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

[18] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 17, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

75. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[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."[19]

76. 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—Social Security numbers, dates of birth, and names.

77. 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."[20]

78. 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.

79. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered,

[19] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft

[20] Tim 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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

and also between when PII 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.[21]

Hi-School Fails to Comply with FTC Guidelines

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

81. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[22]

82. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity

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

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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[23]

83. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

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

85. These FTC enforcement actions include actions against employers over the compromised PII of its employees, like Hi-School here.

86. Hi-School failed to properly implement basic data security practices.

87. Hi-School's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

88. Upon information and belief, Hi-School was at all times fully aware of its obligation to protect the PII of its employees. Hi-School was also aware of the significant repercussions that would result from its failure to do so.

---

[23] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

Hi-School Fails to Comply with Industry Standards

89. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

90. The cybersecurity industry has identified several best practices that a minimum should be implemented by employers in possession of PII, like Hi-School, 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. Hi-School failed to follow these industry best practices, including a failure to implement multi-factor authentication.

91. Other best cybersecurity practices that are standard for employers 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. Hi-School failed to follow these cybersecurity best practices, including failure to train staff.

92. Hi-School failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

93. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to its employees with respect to data privacy. Upon information and belief, Hi-School failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries and Damages

94. As a result of Hi-School's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Hi-School's possession and is subject to further unauthorized disclosures so long as Hi-School fails to undertake appropriate and adequate measures to protect the PII.

The Data Breach Increases Plaintiff's and Class Member's Risk of Identity Theft

95. Plaintiff and Class Members are at a present and continued risk of identity theft for years to come.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

96. The unencrypted PII of Class Members has or will be available for sale on the dark web because that is the *modus operandi* of hackers.

97. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members.

98. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

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

100. 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.

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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

102. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[24]

103. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII 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.

104. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' 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 that was exfiltrated in the Data Breach, criminals may still 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.

[24] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

105. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

106. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

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

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

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

109. Thus, due to the actual and imminent risk of identity theft that Plaintiff and Class Members face, Hi-School's Notice Letter instructs Plaintiffs and Class Members to do the following: "[w]e recommend that you remain vigilant by reviewing your account statements and credit reports closely."[25]

110. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of

[25] Notice Letter.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

the Data Breach and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

111. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[26]

112. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach 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.[27]

113. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[28]

---

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

[27] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

Diminution Value of PII

114. PII is a valuable property right.[29] Considering the value of Big Data in corporate America, and the fact that the consequences of cyber thefts include heavy prison sentences, its value is axiomatic. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

115. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other entities in custody of PII often purchase PII on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims herself. Insurance companies purchase and use wrongfully disclosed PII to adjust their insureds' medical insurance premiums.

116. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[30] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[31,32]

117. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[33]

---

[29] *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).

[30] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[31] https://datacoup.com/

[32] https://digi.me/what-is-digime/

[33] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

118. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[34]

119. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

120. 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, e.g., Social Security numbers, dates of birth, and names.

121. 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.

122. The fraudulent activity resulting from the Data Breach may not come to light for years.

123. At all relevant times, Hi-School knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Hi-School's data security system was

[34] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

124. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

125. Hi-School was, or should have been, fully aware of the unique type and the significant volume of data on Hi-School's network, amounting to more than seventeen thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

126. The injuries to Plaintiff and Class Members were directly and proximately caused by Hi-School's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Costs of Credit and Identity Theft Monitoring is Reasonable and Necessary

127. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of PII accessed in the Data Breach, 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 PII for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

129. 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.

130. 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.[35] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

131. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

132. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Hi-School's Data Breach.

Loss of Benefit of the Bargain

133. Furthermore, Hi-School's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to obtain employment at Hi-School under certain terms, Plaintiff and other reasonable employees understood and expected that Hi-School would properly safeguard and protect their PII, when in fact, Hi-School did not provide the expected data security. Accordingly, Plaintiff and Class Members received

[35] *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.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

employment positions of a lesser value than what they reasonably expected to receive under the bargains they struck with Hi-School.

Plaintiff Shayna Marie Landin's Experience

134. Plaintiff Landin is a former employee at Hi-School who worked there until approximately 2017.

135. As a condition of her employment at Hi-School, she was required to supply Hi-School with her PII, including but not limited to her name, date of birth, and Social Security number.

136. Plaintiff Landin is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

137. At the time of the Data Breach—on or around November 3, 2023—Hi-School retained Plaintiff's PII in its systems.

138. Plaintiff Landin received the Notice Letter, by U.S. mail, directly from Hi-School, dated December 5, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her full name, date of birth, and Social Security number.

139. As a result of the Data Breach, and at the direction of Hi-School's Notice Letter, which instructs Plaintiff to "remain vigilant by reviewing your account statements and credit reports closely,"[36] Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach and monitoring her financial accounts for any indication of fraudulent activity, which

[36] Notice Letter.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

may take years to detect. Plaintiff has spent significant on mitigation activities in response to the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

140. Subsequent to the Data Breach, Plaintiff Landin has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (vii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Hi-School's possession and is subject to further unauthorized disclosures so long as Hi-School fails to undertake appropriate and adequate measures to protect the PII.

141. Plaintiff also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

142. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Hi-School has still not fully informed her of key details about the Data Breach's occurrence.

143. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

144. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

145. Plaintiff Landin has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Hi-School's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

146. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

147. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **Nationwide Class**
> All individuals in the United States whose PII was impacted as a result of the Data Breach (the "Class").

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

149. Plaintiff hereby reserves the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

150. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, according to the reports submitted to the Maine Attorney General, the Class consists of approximately 17,000 individuals whose data was compromised in Data Breach.[37]

[37] https://apps.web.maine.gov/online/aeviewer/ME/40/47edbdd7-acf2-428a-9440-

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

151. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Hi-School unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Hi-School failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Hi-School's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

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

e. Whether Hi-School owed a duty to Class Members to safeguard their PII;

f. Whether Hi-School breached its duty to Class Members to safeguard their PII;

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

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

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Hi-School's misconduct;

j. Whether Hi-School's conduct was negligent;

k. Whether Hi-School breached implied contracts for adequate data security with Plaintiff and Class Members;

4f1ffccce7a0.shtml

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

l. Whether Hi-School was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiff and Class Members;

m. Whether Hi-School's conduct was unfair or deceptive in a manner that might impact the public interest;

n. Whether Hi-School failed to provide notice of the Data Breach in a timely manner; and,

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

152. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

153. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

154. Predominance. Hi-School has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' PII was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Hi-School's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

155. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Hi-School. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

156. Hi-School has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

157. Likewise, particular issues under Fed. R. Civ. P. 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 Hi-School owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

b. Whether Hi-School's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Hi-School's failure to institute adequate protective security measures amounted to negligence;

d. Whether Hi-School's conduct was unfair or deceptive in a manner that might impact the public interest;

e. Whether Hi-School failed to take commercially reasonable steps to safeguard consumer PII; and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

158. Finally, all Members of the proposed Class are readily ascertainable. Hi-School has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by Hi-School.

COUNT I
Negligence
(On behalf of Plaintiff and the Class)

159. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

160. Hi-School requires its employees, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of providing its services.

161. Hi-School gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its employees, which solicitations and services affect commerce.

162. Plaintiff and Class Members entrusted Hi-School with their PII with the understanding that Hi-School would safeguard their information.

163. Hi-School had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

164. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Hi-School had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

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

166. Hi-School owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

167. Hi-School's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Hi-School and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Hi-School with their confidential PII, a necessary part of obtaining employment at Hi-School.

168. Hi-School's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Hi-School is bound by industry standards to protect confidential PII.

169. Hi-School was subject to an "independent duty," untethered to any contract between Hi-School and Plaintiff or the Class.

170. Hi-School also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII it was no longer required to retain pursuant to regulations.

171. Moreover, Hi-School had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

172. Hi-School had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Hi-School's possession might have been compromised, how

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

173. Hi-School breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Hi-School include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

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

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove former employees' PII it was no longer required to retain pursuant to regulations,

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

174. Hi-School violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Hi-School's conduct was particularly unreasonable given the nature and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

175. Hi-School's violation of Section 5 of the FTC Act constitutes negligence.

176. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statute was intended to guard against.

177. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

178. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Hi-School's inadequate security practices.

179. It was foreseeable that Hi-School's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting employers in possession of PII.

180. Hi-School has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

181. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Hi-School knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Hi-School's systems.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

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

183. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Hi-School's possession.

184. Hi-School was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

185. Hi-School's duty extended to protecting Plaintiff 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 have also recognized the existence of a specific duty to reasonably safeguard personal information.

186. Hi-School has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

187. But for Hi-School's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

188. There is a close causal connection between Hi-School's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Hi-School's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

189. As a direct and proximate result of Hi-School's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Hi-School's possession and is subject to further unauthorized disclosures so long as Hi-School fails to undertake appropriate and adequate measures to protect the PII.

190. As a direct and proximate result of Hi-School's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

191. Additionally, as a direct and proximate result of Hi-School's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Hi-School's possession and is subject to further unauthorized disclosures so long as Hi-School fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

193. Hi-School's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

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

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

195. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

196. Plaintiff and Class Members were required to provide their PII to Hi-School as a condition of obtaining employment at Hi-School.

197. Plaintiff and the Class entrusted their PII to Hi-School. In so doing, Plaintiff and the Class entered into implied contracts with Hi-School by which Hi-School agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

198. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Hi-School's data security practices complied with relevant laws and regulations and were consistent with industry standards.

199. Implicit in the agreement between Plaintiff and Class Members and the Hi-School to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

200. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Hi-School, on the other, is demonstrated by their conduct and course of dealing.

201. Hi-School solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of Hi-School's regular business practices. Plaintiff and Class Members accepted Hi-School's offers and provided their PII to Hi-School.

202. In accepting the PII of Plaintiff and Class Members, Hi-School understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

203. On information and belief, at all relevant times Hi-School promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

204. On information and belief, Hi-School further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

205. Plaintiff and Class Members provided their labor and PII to Hi-School with the reasonable belief and expectation that Hi-School would use part of its earnings to obtain adequate data security. Hi-School failed to do so.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

206. Plaintiff and Class Members would not have entrusted their PII to Hi-School in the absence of the implied contract between them and Hi-School to keep their information reasonably secure.

207. Plaintiff and Class Members would not have entrusted their PII to Hi-School in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

208. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Hi-School.

209. Hi-School breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

210. As a direct and proximate result of Hi-School's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

211. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

212. Plaintiff and Class Members are also entitled to injunctive relief requiring Hi-School to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

213. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

214. Plaintiff pleads this claim in the alternative to her contract claim above (Count II).

215. Plaintiff and Class Members conferred a monetary benefit on Hi-School by providing Hi-School with their labor and/or their PII to Hi-School.

216. Hi-School appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

217. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Hi-School to retain that benefit without payment of the value thereof.

218. Specifically, Hi-School enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Hi-School instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Hi-School's decision to prioritize its own profits over the requisite data security.

219. Under principles of equity and good conscience, Hi-School should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members, because Hi-School failed to implement appropriate data management and security measures.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

220. Hi-School acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

221. If Plaintiff and Class Members knew that Hi-School had not secured their PII, they would not have agreed to provide their PII to Hi-School.

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

223. As a direct and proximate result of Hi-School's conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Hi-School's possession and is subject to further unauthorized disclosures so long as Hi-School fails to undertake appropriate and adequate measures to protect the PII.

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

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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

COUNT IV
Violation Of The Washington Consumer Protection Act
Wash. Rev. Code § 19.86.020, *et seq.*
(On Behalf of Plaintiff and the Class)

226. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

227. Plaintiff and Class members are "persons" under the Washington Consumer Protection Act. RCW 19.86.010(1).

228. Hi-School is a "person" as described in the Washington Consumer Protection Act. RCW 19.86.010(1).

229. Hi-School is engaged in, and its acts and omissions affect, trade and commerce. Hi-School's relevant acts, practices, and omissions complained of in this action were done in the course of Hi-School's business of marketing, offering for sale, and selling services throughout Washington and the United States.

230. Hi-School is headquartered in Washington; its strategies, decision-making, and commercial transactions originate in Washington; most of its key operations and employees reside, work, and make company decisions (including data security decisions) in Washington; and many of its employees are residents of the State of Washington.

231. The Washington Consumer Protection Act prohibits deceptive and unfair acts or practices in the conduct of any business, trade, or commerce, or in the provision of commerce. RCW 19.86.020.

232. In the course of conducting its business, Hi-School committed "unfair acts or practices" by, *inter alia,* knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

Members' PII. Such practices were likely to cause substantial injury to consumers and were, not reasonably avoidable by consumers and nor outweighed by countervailing benefits.

233. Hi-School's conduct was also deceptive. Hi-School failed to timely notify and concealed from Plaintiff and Class Members the inadequacy of its data security measures and the unauthorized release and disclosure of their PII. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII and identities.

234. Hi-School's unfair and deceptive acts or practices in the conduct of business include, but are not limited to:

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

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII;

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

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII; and

h. Failing to promptly and adequately notify Plaintiff and the Class that their PII was accessed by unauthorized persons in the Data Breach.

235. Hi-School's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as the FTC Act.

236. The injuries suffered by Plaintiff and the Class greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiff and the Class should or could have reasonably avoided.

237. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and the Class as a direct and proximate result of Hi-School's unfair and deceptive acts and practices as set forth herein include: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Hi-School's possession and is subject to further unauthorized disclosures so long as Hi-School fails to undertake appropriate and adequate measures to protect the PII.

238. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Hi-School from disclosing their PII without their consent and prohibiting Hi-School from continuing its wrongful conduct; reasonable attorneys' fees and costs; treble damages for each Class member, not to exceed $25,000 per Class member; and any other relief that is just and proper under RCW 19.86.090.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Hi-School and that the Court grants the following:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For equitable relief enjoining Hi-School from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

i. prohibiting Hi-School from engaging in the wrongful and unlawful acts described herein;

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

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

iv. requiring Hi-School to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Hi-School from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

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

viii. requiring Hi-School to audit, test, and train their security personnel regarding any new or modified procedures; requiring Hi-School to segment data by, among other things, creating firewalls and access controls so that if one area of Hi-School's network is compromised, hackers cannot gain access to other portions of Hi-School's systems;

ix. requiring Hi-School to conduct regular database scanning and securing checks;

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

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

xii. requiring Hi-School to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Hi-School's policies,

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

programs, and systems for protecting personal identifying information;

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

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

xv. requiring Hi-School to implement logging and monitoring programs sufficient to track traffic to and from Hi-School's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Hi-School's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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

E. For an award of punitive damages, as allowable by law;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
TEL. 206.682.5600 • FAX 206.682.2992

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

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

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated: February 12, 2024

Respectfully submitted,

TOUSLEY BRAIN STEPHENS PLLC

s/Jason T. Dennett
Jason T. Dennett, WSBA No. 30686
s/Kaleigh N. Boyd
Kaleigh N. Boyd, WSBA No. 52684
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Phone: (206) 682-5600
jdennett@tousley.com
kboyd@tousley.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Counsel for Plaintiff and the Proposed Class

**Pro Hac Vice* application forthcoming

ClassAction.org