Honorable Jamal N. Whitehead

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

IN RE: ABC LEGAL SERVICES DATA SECURITY LITIGATION This Document Relates To: All Actions	Master File No. 2:24-cv-02092 **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Anthony Crowley, Steven Sanchez, Kaylee Rinne, Samantha Bodtker, Teresa Bushek, Jeff Hoffman, Craig Vann, and James Munger (collectively, "Plaintiffs"), individually and on behalf of all other similarly situated individuals, and by and through their undersigned counsel, file this Consolidated Class Action Complaint against Defendant ABC Legal Services, LLC ("ABC Legal" or "Defendant") and allege the following based upon their personal knowledge of the facts, information and belief, and the investigation of their counsel.

I. INTRODUCTION

1. Plaintiffs bring this class action lawsuit against ABC Legal for its failure to protect and safeguard Plaintiffs' and the Class's highly sensitive personally identifiable information ("PII") culminating in a massive and preventable data breach impacting at least **39,965**

individuals (the "Data Breach" or "Breach").[1] As a result of ABC Legal's insufficient data security, cybercriminals easily infiltrated ABC Legal's inadequately protected computer network and stole the PII of Plaintiffs and the Class.[2]

2. ABC Legal provides legal solutions to its customers, including law firms, businesses, and individuals.[3]

3. ABC Legal's services include service of process, e-filing, and skip tracing.[4]

4. In conjunction with services ABC Legal provides, ABC Legal obtains and collects PII from its customers.[5]

5. ABC Legal also acquires the PII of its employees and contractors.

6. According to ABC Legal, on August 7, 2024, it detected unusual activity in its network environment.[6]

7. Despite detecting the Data Breach on August 7, 2024, ABC Legal did not regain control of its network environment until August 8, 2024.[7]

8. After an investigation, ABC Legal determined that "**certain files were likely taken from [its] network on August 7, 2024**."[8]

---

[1] *See* OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications*, ABC Legal Services, LLC, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b7f2187e-3ceb-4f2e-b48e-f697fdd84918.html (last visited Mar. 10, 2025) (the Maine Attorney General's website previously stated the number of persons impacted by the Data Breach was 39,965; however, this number has since been removed from the website).

[2] *See id.* (containing a link to a sample of the consumer notification letter Defendant issued to Data Breach victims such as Plaintiff and the Class).

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Id.* (emphasis added).

9. The stolen files contained the PII of Plaintiffs and the Class.[9]

10. The types of confidential PII accessed and acquired in the Data Breach included Plaintiffs' and the Class's: names, Social Security numbers, driver's license numbers, government-issued ID numbers (e.g., passports and state ID cards), financial information (e.g., account numbers and credit or debit card numbers), health insurance information, and dates of birth (collectively, "Private Information").[10]

11. As a result of ABC Legal's inadequately secured computer network, Plaintiffs and Class Members have had their Private Information accessed and stolen.

12. ABC Legal failed to uphold its data security obligations to Plaintiffs and Class Members by failing to properly safeguard and protect their Private Information, thereby enabling cybercriminals to steal it.

13. Due to ABC Legal's negligence, Plaintiffs and the Class will face an imminent risk of identity theft and fraud for the rest of their lives. Indeed, the threat of harm has already materialized because ABC Legal acknowledged that the Private Information of Plaintiffs and the Class was likely stolen.[11] For the rest of their lives, Plaintiffs and Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information.

14. Plaintiffs and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their PII, and/or additional damages as described herein.

15. Plaintiffs bring this action individually and on behalf of the Class, seeking

---

[9] *Id.*

[10] *Data Security Breach Reports*, ATTORNEY GENEAL OF TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Mar. 10, 2025) (search for "ABC Legal Services, Inc.").

[11] OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications*, ABC Legal Services, LLC, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b7f2187e-3ceb-4f2e-b48e-f697fdd84918.html (last visited Mar. 10, 2025).

remedies including, but not limited to, compensatory damages, nominal damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

16. Plaintiff **Anthony Crowley** is a resident and citizen of the State of Texas.

17. Plaintiff **Steven Sanchez** is a resident and citizen of the State of New York.

18. Plaintiff **Kaylee Rinne** is a resident and citizen of the State of Oregon.

19. Plaintiff **Samantha Bodtker** is a resident and citizen of the State of Oregon.

20. Plaintiff **Teresa Bushek** is a resident and citizen of the State of Texas.

21. Plaintiff **Jeff Hoffman** is a resident and citizen of the State of Minnesota.

22. Plaintiff **Craig Vann** is a resident and citizen of the State of Alabama.

23. Plaintiff **James Munger** is a resident and citizen of the State of Washington.

24. Defendant **ABC Legal Services, LLC** is a Washington limited liability company with its principal place of business located at 1099 Stewart St., Suite 700, Seattle, WA 98101.

III. JURISDICTION AND VENUE

25. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

26. This Court has personal jurisdiction over Defendant because it is headquartered in and/or operates within this District and regularly transacts business, has agents, and is otherwise within this District.

27. Venue is likewise proper as to Defendant in this District because a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2).

IV. FACTUAL ALLEGATIONS

A. ABC Legal's Services.

28. ABC Legal was established in 1974 and is headquartered in Seattle, Washington.[12]

29. ABC Legal has over 600 employees across the United States of America.[13]

30. ABC Legal provides legal solutions such as service of process, e-filing, skip tracing, appearance counsel, and venue selection to the customers it services.[14]

31. ABC Legal claims it has the nation's largest network of process servers, delivering service of process in all 50 states and in 77 countries.[15]

32. ABC Legal touts that "[s]ince 2003, the U.S. Department of Justice has delegated its function as the Central Authority to ABC Legal to execute requests for service of judicial and extrajudicial documents in civil and commercial matters directed at private individuals and companies in the United States. ABC Legal manages all formal requests for service of judicial and extrajudicial documents pursuant to the Hague Service Convention and letters rogatory service requests received through diplomatic channels."[16]

33. Due to its prominence in the legal industry, ABC Legal has an estimated annual revenue of $105 million.[17] In other words, ABC Legal had adequate funds available to implement industry standard data security but deliberately chose not to. Instead, ABC Legal unjustly enriched itself with the cost savings of choosing not to employ industry standard data security

---

[12] *About*, ABC LEGAL, https://www.abclegal.com/about (last visited Mar. 10, 2025).

[13] *Id.*

[14] *Id.*

[15] *Serve with Us*, ABC LEGAL, https://www.abclegal.com/serve (last visited Mar. 10, 2025).

[16] *ABC Legal Secures Fifth Consecutive DOJ Contract for International Service of Process*, ABC LEGAL (Feb. 21, 2025), https://www.abclegal.com/blog/abc-legal-secures-fifth-consecutive-doj-contract-for-international-service-of-process (last visited Mar. 10, 2025).

[17] *ABC Legal Services*, ZOOMINFO, https://www.zoominfo.com/c/abc-legal-services-inc/283091 (last visited Mar. 10, 2025).

measures at the expense of Plaintiffs and the Class.

34. In conjunction with the services and employment ABC Legal provides, it is entrusted with the extremely sensitive Private Information of Plaintiffs and the Class.

35. By collecting the PII of Plaintiffs and the Class, ABC Legal undertook a duty to safeguard and protect Plaintiffs' and the Class's Private Information.

36. Indeed, ABC Legal recognized it had a duty to protect Plaintiffs' and the Class's Private Information from unauthorized access and states in its Privacy Policy, "ABC Legal is committed to ensuring that your privacy is protected."[18]

37. ABC Legal further states:

> Security
>
> We are committed to ensuring that your information is secure. In order to prevent unauthorized access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online.[19]

38. Despite recognizing ABC Legal had a duty to keep Plaintiffs' and the Class's Private Information secure, ABC Legal failed to implement industry standard data security infrastructure, software, and encryption resulting in a massive and preventable Data Breach.

B. ABC Legal's Massive and Preventable Data Breach.

39. On August 7, 2024, ABC Legal discovered unusual activity within its network environment.[20]

40. After conducting an investigation, ABC Legal divulged certain files were likely stolen from its network by an unauthorized actor on August 7, 2024.[21]

---

[18] *Privacy Policy*, ABC LEGAL, https://www.abclegal.com/privacy (last visited Mar. 10, 2025).

[19] *Id.*

[20] OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications*, ABC Legal Services, LLC, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b7f2187e-3ceb-4f2e-b48e-f697fdd84918.html (last visited Mar. 10, 2025).

[21] *Id.*

41. The confidential information accessed and acquired in the Data Breach included Plaintiffs' and the Class's: names, Social Security numbers, driver's license numbers, government-issued ID numbers (e.g., passports and state ID cards), financial information (e.g., account numbers and credit or debit card numbers), health insurance information, and dates of birth.[22] In other words, cybercriminals obtained everything they could possibly want to commit identity theft and fraud and wreak havoc on the financial and personal lives of Plaintiffs and the Class.

42. Despite discovering the Breach on August 7, 2024, ABC Legal did not provide notice of the Data Breach to the victims until December 2024, when it sent Notice of Data Breach Letters ("Notice Letters").[23]

43. The Notice Letters obfuscated the nature of the Breach by urging Class Members to sign up for credit monitoring services, place a fraud alert on their credit or freeze their credit, and review their accounts, while also claiming ABC Legal was not aware of any improper use of the stolen Private Information.[24] What ABC Legal fails to realize is that unauthorized access and theft of Plaintiffs' and the Class's Private Information is "improper use" of their Private Information.

C. ABC Legal Admitted it Had Insufficient Data Security After the Breach.

44. Ironically, after the Data Breach, ABC Legal publicly announced that it had achieved "SOC 2 Certification."[25]

---

[22] *Data Security Breach Reports*, ATTORNEY GENERAL OF TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Mar. 10, 2025) (search for "ABC Legal Services, Inc.").

[23] OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications*, ABC Legal Services, LLC, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b7f2187e-3ceb-4f2e-b48e-f697fdd84918.html (last visited Mar. 10, 2025).

[24] *Id.*

[25] *ABC Legal Achieves SOC 2 Certification*, ABC LEGAL (Jan. 30, 2025), https://www.abclegal.com/blog/abc-legal-achieves-soc-2-certification-reaffirming-its-dedication-to-data-security (last visited Mar. 10, 2025).

45. "SOC 2," which stands for "Service Organization Control Type 2," is a cybersecurity compliance framework developed by the American Institute of Certified Public Accountants.[26]

46. The primary purpose of SOC 2 is to ensure that third-party service providers store and process client data in a secure manner.[27]

47. By ABC Legal announcing after the Data Breach that it had achieved SOC 2 certification for the first time, ABC Legal effectively admitted that it had inadequate data security prior to the Data Breach.

48. Altogether, ABC Legal utterly failed to take the necessary precautions required to safeguard and protect Plaintiffs' and the other Class Members' PII from unauthorized access.

49. Plaintiffs have been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PII stolen in the Data Breach.

50. ABC Legal's actions represent a flagrant disregard of the rights of the Class Members, both as to their privacy and their property.

D. Plaintiffs' Experiences.

Plaintiff Steven Sanchez

51. Plaintiff Sanchez was an employee of Defendant's and provided his Private Information to Defendant as a condition of his employment, which was then entered into Defendant's computer system and maintained by Defendant.

52. Plaintiff Sanchez reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data

[26] *What is SOC 2?*, ONELOGIN, https://www.onelogin.com/learn/what-is-soc-2 (last visited Mar. 10, 2025).

[27] *Id.*

breach. Plaintiff Sanchez would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

53. Plaintiff Sanchez received a Notice Letter, dated December 6, 2024, from Defendant informing him that his Private Information had been compromised in the Data Breach. The Notice Letter stated that at least Plaintiff Sanchez's full name and Social Security number was accessed in the Data Breach.

54. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Sanchez faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice Letter Plaintiff Sanchez received also cautioned him to "remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."

55. Plaintiff Sanchez greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Sanchez is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

56. Plaintiff Sanchez stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

57. To Plaintiff Sanchez's knowledge, his PII has not been compromised in a prior data breach.

58. As a result of the Data Breach, Plaintiff Sanchez has spent numerous hours researching the Data Breach, verifying the legitimacy of the Notice Letter, signing up for the credit monitoring service, reviewing his bank accounts, monitoring his credit report, changing

his passwords and payment account numbers, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

59. As a consequence of and following the Data Breach, Plaintiff Sanchez has experienced a large number of spam calls.

60. The Data Breach has caused Plaintiff Sanchez to suffer fear, anxiety, and stress, which has been compounded by Defendant's four-month delay in noticing him of the fact that his Social Security number in conjunction with his date of birth was acquired by criminals as a result of the Data Breach.

61. Plaintiff Sanchez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Sanchez will continue to be at present and continued increased risk of identity theft and fraud for years to come.

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

63. As a direct and traceable result of the Data Breach, Plaintiff Sanchez suffered actual injury and damages, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of his bargain because ABC Legal did not adequately protect his PII; (d) emotional distress because identity thieves now possess his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and likely published on the dark web; (f) diminution in the value of his PII, a form of intangible property that ABC obtained from Plaintiff Sanchez; and (g) other economic and non-economic harm.

Plaintiff Anthony Crowley

64. Plaintiff Crowley was a contractor of Defendant's and provided his Private Information to Defendant as a condition of his employment, which was then entered into Defendant's computer system and maintained by Defendant.

65. Plaintiff Crowley reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Crowley would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

66. Plaintiff Crowley received a Notice Letter, dated December 6, 2024, from Defendant informing him that his Private Information had been compromised in the Data Breach. The Notice Letter stated that Plaintiff Crowley's email address and Social Security number was accessed in the Data Breach.

67. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Crowley faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice Letter Plaintiff Crowley received also cautioned him to "remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."

68. Plaintiff Crowley greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Crowley is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

69. Plaintiff Crowley stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and

passwords for his various online accounts.

70. To Plaintiff Crowley's knowledge, his PII has not been compromised in a prior data breach.

71. As a result of the Data Breach, Plaintiff Crowley has spent numerous hours researching the Data Breach, verifying the legitimacy of the Notice Letter, signing up for the credit monitoring service, reviewing his bank accounts, monitoring his credit report, changing his passwords and payment account numbers, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

72. As a consequence of and following the Data Breach, Plaintiff Crowley has experienced a large number of spam calls.

73. The Data Breach has caused Plaintiff Crowley to suffer fear, anxiety, and stress, which has been compounded by Defendant's four-month delay in noticing him of the fact that his Social Security number in conjunction with his date of birth was acquired by criminals as a result of the Data Breach.

74. Plaintiff Crowley anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Crowley will continue to be at present and continued increased risk of identity theft and fraud for years to come.

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

76. As a direct and traceable result of the Data Breach, Plaintiff Crowley suffered actual injury and damages, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of his bargain because ABC Legal did not adequately protect his PII; (d) emotional distress because identity thieves

now possess his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and likely published on the dark web; (f) diminution in the value of his PII, a form of intangible property that ABC obtained from Plaintiff Crowley; and (g) other economic and non-economic harm.

Plaintiff Kaylee Rinne

77. Plaintiff Rinne provided her Private Information to Defendant as a condition of receiving services from Defendant, which was then entered into Defendant's computer system and maintained by Defendant.

78. Plaintiff Rinne reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Rinne would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

79. Plaintiff Rinne received a Notice Letter dated December 6, 2024, from Defendant informing her that her Private Information had been compromised in the Data Breach. The Notice Letter stated that Plaintiff Rinne's date of birth, Social Security number, and health insurance information were accessed in the Data Breach.

80. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Rinne faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice Letter Plaintiff Rinne received also cautioned her to "remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."

81. Plaintiff Rinne greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Rinne is very

concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

82. Plaintiff Rinne stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

83. To Plaintiff Rinne's knowledge, her PII has not been compromised in a prior data breach.

84. As a result of the Data Breach, Plaintiff Rinne has spent approximately 35 hours researching the Data Breach, verifying the legitimacy of the Notice Letter, reviewing her bank accounts, monitoring her credit report, changing her passwords and payment account numbers, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

85. The Data Breach has caused Plaintiff Rinne to suffer fear, anxiety, and stress, which has been compounded by Defendant's four-month delay in noticing her of the fact that her Social Security number in conjunction with Plaintiff Rinne's date of birth was acquired by criminals as a result of the Data Breach.

86. Plaintiff Rinne anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Rinne will continue to be at present and continued increased risk of identity theft and fraud for years to come.

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

88. As a direct and traceable result of the Data Breach, Plaintiff Rinne suffered actual injury and damages, including, but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of her bargain because ABC Legal did not adequately protect her PII; (d) emotional distress because identity thieves now possess her Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII has been stolen and likely published on the dark web; (f) diminution in the value of her PII, a form of intangible property that ABC obtained from Plaintiff Rinne; and (g) other economic and non-economic harm.

Plaintiff Samantha Bodtker

89. Plaintiff Bodtker was an employee of Defendant and provided her Private Information to Defendant as a condition of her employment, which was entered into Defendant's computer system and maintained by Defendant.

90. Plaintiff Bodtker reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Bodtker would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

91. Plaintiff Bodtker received a Notice Letter, dated December 6, 2024, from Defendant informing her that her Private Information had been compromised in the Data Breach. The Notice Letter stated that Plaintiff Bodtker's email address and Social Security number were accessed in the Data Breach.

92. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Bodtker faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice Letter Plaintiff Bodtker received also cautioned her to "remain vigilant in

reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."

93. Plaintiff Bodtker greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Bodtker is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

94. Plaintiff Bodtker stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

95. To Plaintiff Bodtker's knowledge, her PII has not been compromised in a prior data breach.

96. As a result of the Data Breach, Plaintiff Bodtker has spent several hours per week on activities including researching the Data Breach, verifying the legitimacy of the Notice Letter, reviewing her bank accounts, monitoring her credit report, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

97. As a consequence of and following the Data Breach, Plaintiff Bodtker has experienced a drastic increase in unsolicited and spam phone calls and emails.

98. The Data Breach has caused Plaintiff Bodtker to suffer fear, anxiety, and stress, which has been compounded by Defendant's four-month delay in noticing her of the fact that her Social Security number in conjunction with her email address was acquired by criminals as a result of the Data Breach.

99. Plaintiff Bodtker anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition,

Plaintiff Bodtker will continue to be at present and continued increased risk of identity theft and fraud for years to come.

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

101. As a direct and traceable result of the Data Breach, Plaintiff Bodtker suffered actual injury and damages, including, but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of her bargain because ABC Legal did not adequately protect her PII; (d) emotional distress because identity thieves now possess her Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII has been stolen and likely published on the dark web; (f) diminution in the value of her PII, a form of intangible property that ABC obtained from Plaintiff Bodtker; and (g) other economic and non-economic harm.

Plaintiff Teresa Bushek

102. Plaintiff Bushek was a contractor of Defendant's and provided her Private Information to Defendant as a condition of being a contractor for Defendant, which was then entered into Defendant's computer system and maintained by Defendant.

103. Plaintiff Bushek reasonably understood and expected that Defendant would safeguard her Private Information and timely and adequately notify her in the event of a data breach. Plaintiff Bushek would not have allowed Defendant, or anyone in Defendant's position, to maintain her Private Information if she believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

104. Plaintiff Bushek received a Notice Letter, dated December 6, 2024, from Defendant informing her that her Private Information had been compromised in the Data Breach.

The Notice Letter stated that Plaintiff Bushek's email address and Social Security number were accessed in the Data Breach.

105. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Bushek faces, Defendant offered her a twelve-month subscription to a credit monitoring service. The Notice Letter Plaintiff Bushek received also cautioned her to "remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."

106. Plaintiff Bushek greatly values her privacy and Private Information and takes reasonable steps to maintain the confidentiality of her Private Information. Plaintiff Bushek is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

107. Plaintiff Bushek stores any and all documents containing Private Information in a secure location and destroys any documents she receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

108. To Plaintiff Bushek's knowledge, her PII has not been compromised in a prior data breach.

109. As a result of the Data Breach, Plaintiff Bushek has spent hours researching the Data Breach, verifying the legitimacy of the Notice Letter, reviewing her bank accounts, monitoring her credit report and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

110. As a direct result of the Data Breach, Plaintiff Bushek has been inundated with unsolicited and burdensome spam emails. These unsolicited spam emails are not a coincidence. Defendant admitted in the Notice Letter sent to Plaintiff Bushek that her email address was compromised in the Data Breach, which provides a direct causal link.

111. The Data Breach has caused Plaintiff Bushek to suffer fear, anxiety, and stress, which has been compounded by Defendant's four-month delay in noticing her of the fact that her Social Security number was acquired by criminals as a result of the Data Breach.

112. Plaintiff Bushek anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Bushek will continue to be at present and continued increased risk of identity theft and fraud for years to come.

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

114. As a direct and traceable result of the Data Breach, Plaintiff Bushek suffered actual injury and damages, including, but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her PII being accessed and stolen by cybercriminals; (c) loss of the benefit of her bargain because ABC Legal did not adequately protect her PII; (d) emotional distress because identity thieves now possess her Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her PII has been stolen and likely published on the dark web; (f) diminution in the value of her PII, a form of intangible property that ABC obtained from Plaintiff Bushek; and (g) other economic and non-economic harm.

Plaintiff Jeff Hoffman

115. Plaintiff Hoffman provided his Private Information to Defendant as a condition of receiving services from Defendant, which was then entered into Defendant's computer system and maintained by Defendant.

116. Plaintiff Hoffman reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data

breach. Plaintiff Hoffman would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

117. Plaintiff Hoffman received a Notice letter dated December 6, 2024, from Defendant informing him that his Private information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Hoffman's Taxpayer ID Number was accessed in the Data Breach.

118. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Hoffman faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Hoffman received also cautioned him to "remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."

119. Plaintiff Hoffman greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Hoffman is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

120. Plaintiff Hoffman stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

121. As a result of the Data Breach, Plaintiff Hoffman has spent approximately two

and a half hours verifying the legitimacy of the Notice letter, reviewing his bank accounts, monitoring his credit report, changing his passwords, and other necessary mitigation efforts. This is valuable time that Plaintiff Hoffman spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

122. As a consequence of and following the Data Breach, Plaintiff Hoffman has experienced attempts at breaching several of his online accounts, such as Apple, Uber, and Venmo. Additionally, Plaintiff Hoffman has experienced a significant increase in the number of spam emails, phishing scams, and junk phone calls/texts.

123. The Data Breach has caused Plaintiff Hoffman to suffer fear, anxiety, and stress, which has been compounded by Defendant's four-month delay in noticing him of the fact that his Taxpayer ID number was acquired by criminals as a result of the Data Breach.

124. Plaintiff Hoffman anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Hoffman will continue to be at present and continued increased risk of identity theft and fraud for years to come.

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

126. As a direct and traceable result of the Data Breach, Plaintiff Hoffman suffered actual injury and damages, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of his bargain because ABC Legal did not adequately protect his PII; (d) emotional distress because identity thieves now possess his Social Security number and other sensitive information; (e) imminent and

impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and likely published on the dark web; (f) diminution in the value of his PII, a form of intangible property that ABC obtained from Plaintiff Hoffman; and (g) other economic and non-economic harm.

Plaintiff Craig Vann

127. Plaintiff Vann was an employee of Defendant's and provided his Private Information to Defendant as a condition of his employment, which was then entered into Defendant's computer system and maintained by Defendant.

128. Plaintiff Vann reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Vann would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

129. Plaintiff Vann received a Notice letter dated December 6, 2024, from Defendant informing him that his Private information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Vann's full name, date of birth, email address, Social Security number, and health insurance information were accessed in the Data Breach.

130. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Vann faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Vann received also cautioned him to "remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."

131. Plaintiff Vann greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Vann is very concerned about identity theft and fraud, as well as the consequences of such identity theft and

fraud resulting from the Data Breach.

132. Plaintiff Vann stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

133. To Plaintiff Vann's knowledge, his PII has not been compromised in a prior data breach.

134. As a result of the Data Breach, Plaintiff Vann has spent approximately 2 hours researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for the credit monitoring service, reviewing his bank accounts, monitoring his credit report, changing his passwords and payment account numbers, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

135. As a consequence of and following the Data Breach, Plaintiff Vann has experienced a false address listed on his credit monitoring service, which he never resided at.

136. The Data Breach has caused Plaintiff Vann to suffer fear, anxiety, and stress, which has been compounded by Defendant's four-month delay in noticing him of the fact that his Social Security number in conjunction with his date of birth was acquired by criminals as a result of the Data Breach.

137. Plaintiff Vann anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Vann will continue to be at present and continued increased risk of identity theft and fraud for years to come.

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

139. As a direct and traceable result of the Data Breach, Plaintiff Vann suffered actual injury and damages, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of his bargain because ABC Legal did not adequately protect his PII; (d) emotional distress because identity thieves now possess his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and likely published on the dark web; (f) diminution in the value of his PII, a form of intangible property that ABC obtained from Plaintiff Vann; and (g) other economic and non-economic harm.

Plaintiff James Munger

140. Plaintiff Munger was an employee of Defendant's and provided his Private Information to Defendant as a condition of his employment which was then entered into Defendant's computer system and maintained by Defendant.

141. Plaintiff Munger reasonably understood and expected that Defendant would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff Munger would not have allowed Defendant, or anyone in Defendant's position, to maintain his Private Information if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

142. Plaintiff Munger received a Notice letter dated December 6, 2024, from Defendant informing him that his Private information had been compromised in the Data Breach. The Notice letter stated that Plaintiff Munger's full name, date of birth, email address, Social Security number and health insurance information was accessed in the Data Breach.

143. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Munger faces, Defendant offered him a twelve-month subscription to a credit monitoring service. The Notice letter Plaintiff Munger received also cautioned him to "remain

vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."

144. Plaintiff Munger greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff Munger is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

145. Plaintiff Munger stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

146. To Plaintiff Munger's knowledge, his PII has not been compromised in a prior data breach.

147. As a result of the Data Breach, Plaintiff Munger has spent approximately 20 hours researching the Data Breach, verifying the legitimacy of the Notice letter, signing up for credit monitoring service, reviewing his bank accounts, monitoring his credit report, changing his passwords and payment account numbers, and other necessary mitigation efforts. This is valuable time that Plaintiff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

148. The Data Breach has caused Plaintiff Munger to suffer fear, anxiety, and stress, which has been compounded by Defendant's four-month delay in noticing him of the fact that his Social Security number in conjunction with his date of birth was acquired by criminals as a result of the Data Breach.

149. Plaintiff Munger anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Munger will continue to be at present and continued increased risk of identity theft and fraud for years to come.

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

151. As a direct and traceable result of the Data Breach, Plaintiff Munger suffered actual injury and damages, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his PII being accessed and stolen by cybercriminals; (c) loss of the benefit of his bargain because ABC Legal did not adequately protect his PII; (d) emotional distress because identity thieves now possess his Social Security number and other sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has been stolen and likely published on the dark web; (f) diminution in the value of his PII, a form of intangible property that ABC obtained from Plaintiff Munger; and (g) other economic and non-economic harm.

E. Cybercriminals Will Use the PII Obtained in the Breach to Defraud Plaintiffs and the Class.

152. PII is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune, including ways already experienced by Plaintiffs as set forth above.

153. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.28 For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names

[28] *See Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Mar. 10, 2025).

to police during arrests, and many other harmful forms of identity theft.29 These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and the Class Members.

154. Social Security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[30]

(Emphasis added).

155. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years to come.31

156. There is no doubt this was a financially motivated breach, as the only reason the perpetrator of the Data Breach would go through the trouble of running a targeted cyberattack against a company like ABC Legal is to get information that it can monetize by selling on the black market for use in the kinds of criminal activity described herein. Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.32 "[I]f

---

[29] *See, e.g.*, *What Can Someone Do With Your Social Security Number?*, CREDIT.COM (Oct. 19, 2023), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Mar. 10, 2025).

[30] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited Mar. 10, 2025).

[31] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), available at: https://www.gao.gov/products/gao-07-737 (last visited Mar. 10, 2025).

[32] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, PC MAG (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last visited Mar. 10, 2025).

there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."33

157. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, they will use it.34

158. Hackers may not have immediate use of the information, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n 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.[35]

159. For instance, with a stolen Social Security number, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.36

160. The ramifications of Defendant's failure to keep Class Members' PII secure are long lasting and severe. Once that information is stolen and compromised, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to twelve months or even longer.

161. Further, criminals often trade stolen PII on the "cyber black-market" for years

---

[33] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (last visited Mar. 10, 2025).

[34] Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info (last visited Mar. 10, 2025).

[35] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), available at: https://www.gao.gov/products/gao-07-737 (last visited Mar. 10, 2025).

[36] *See, e.g.*, *What Can Someone Do With Your Social Security Number?*, CREDIT.COM (Oct. 19, 2023), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Mar. 10, 2025).

following a breach. Cybercriminals can post stolen PII on the internet, thereby making such information publicly available.

162. Most victims do not realize that their identity has been compromised until more than two years after it has happened. This gives thieves ample time to seek multiple medical treatments under the victim's name, among other misuses.

163. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit and protecting themselves in the future.[37]

164. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have had their PII exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of further harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiffs and other Class Members must go through, which can include spending countless hours filing police reports, following Federal Trade Commission checklists, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps.

165. Plaintiffs and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including, but not limited to:

a. Actual identity theft;

b. Trespass, damage to, and theft of their personal property including PII;

c. Improper exposure of their PII;

d. Online publication of their PII on the dark web;

[37] *See Identity Theft Guide for Individuals*, IRS, https://www.irs.gov/identity-theft-fraud-scams/identity-theft-guide-for-individuals (last visited Mar. 10, 2025).

e. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and misused;

f. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cybercriminals have their PII and that identity thieves have likely already used that information to defraud other victims of the Data Breach;

g. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

h. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

i. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class Members' personal information for which there is a well-established and quantifiable national and international market;

j. The loss of use and access to their credit, accounts, and/or funds;

k. Damage to their credit due to fraudulent use of their PII; and/or

l. Increased cost of financing loans, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

166. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiffs' PII.

167. Plaintiffs and Class Members also have an interest in ensuring that their PII that was provided to ABC Legal is removed from ABC Legal's unencrypted files.

168. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiffs and Class Members an inadequate 12 months of identity theft repair and

monitoring services.[38] This limited identity theft monitoring is, however, insufficient to protect Plaintiffs and Class Members from a lifetime of identity theft risk.

169. The Notice Letters further acknowledged that the Data Breach would cause inconvenience including financial harm, to affected individuals and provided numerous actions Class Members could take to mitigate those harms caused by the Data Breach, including placing freezes or fraud alerts on their credit. Indeed, ABC Legal's Notice Letter admonishes victims to "remain vigilant" by "reviewing financial account statements and credit reports for fraudulent or irregular activity on a regular basis."[39]

170. At ABC Legal's suggestion, Plaintiffs are desperately trying to mitigate the damage that ABC Legal has caused them. Given the kind of PII hackers stole from ABC Legal's network, however, Plaintiffs are certain to incur additional damages. Because identity thieves have obtained confidential PII, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and tedious process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[40]

171. None of this should have happened because the Data Breach was preventable.

F. Defendant was Aware of the Risk of Cyber Attacks.

172. Data security breaches have dominated the headlines for the last two decades, and it does not take an IT industry expert to know about it. The general public is aware of some of

---

[38] *See* OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications*, ABC Legal Services, LLC, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b7f2187e-3ceb-4f2e-b48e-f697fdd84918.html (last visited Mar. 10, 2025)

[39] *Id.*

[40] *See What Happens if I Change my Social Security number?*, LEXINGTON LAW (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html (last visited Mar. 10, 2025).

the biggest cybersecurity breaches including Target,[41] Yahoo,[42] Marriott International,[43] Chipotle, Chili's, Arby's,[44] and others.[45]

173. There is a significant prevalence of data breaches in the legal industry. "Data breaches in the legal industry are trending in a concerning direction; the industry faced an average of 1,055 cyberattacks per week in 2023, representing a 13% increase from the previous year. It shouldn't come as a surprise that organizations in the legal field are targeted considering the wealth of sensitive information . . . ."[46]

174. "Legal services providers handle information that is often extremely sensitive. From intellectual property documents to details of criminal cases, the data in possession of these firms is valuable to cybercriminals who may exploit it for financial gain, identity theft, or corporate espionage."[47]

175. ABC Legal knew that cybercriminals routinely target entities within the legal industry in an attempt to steal collected Private Information. Despite this, ABC Legal failed to

---

[41] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015, 8:20 AM PT), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/ (last visited Mar. 10, 2025).

[42] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html (last visited Mar. 10, 2025).

[43] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited Mar. 10, 2025).

[44] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b (last visited Mar. 10, 2025).

[45] *See, e.g.*, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Sept. 12, 2024), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last visited Mar. 10, 2025).

[46] Jack Browning, *Data Breaches in the Legal Industry: is Your Information Safe?*, ONE LEGAL (Feb. 19, 2024) https://www.onelegal.com/blog/data-breaches-in-the-legal-industry/ (last visited Mar. 10, 2025).

[47] *Id.*

and/or chose not to maintain many reasonable and necessary industry standards necessary to prevent data breaches.

176. ABC Legal was clearly aware of the risks and the harm that could result from inadequate date security but failed to implement appropriate data security measures.

G. Defendant Could Have Prevented the Data Breach.

177. Data breaches are preventable.[48] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[49] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[50]

178. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures . . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."[51]

179. In a Data Breach like the one here, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The guidelines also emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[52] The guidelines establish that businesses should protect the confidential information that

---

[48] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[49] *Id.* at 17.

[50] *Id.* at 28.

[51] *Id.*

[52] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited March 10, 2025).

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 for installing vendor-approved patches to correct security problems. The guidelines recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

180. Upon information and belief, ABC Legal failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including those in the FTC's guidelines. ABC Legal also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in cybersecurity readiness.

181. 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."53

182. To prevent and detect cyberattacks, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Since 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.

---

53 *See How to Protect Your Networks from RANSOMWARE*, at 3, available at: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited March 10, 2025).

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices, and use 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 wide access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if not in use.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policies.
- 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.[54]

183. Further, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

[54] *Id.* at 3–4.

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

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

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

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

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

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

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . . .[55]

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

184. In addition, to prevent and detect ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply the latest security updates.
  - Use threat and vulnerability management systems.
  - Perform regular audits and remove privileged credentials.
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as full potential compromises.
- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely.
- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords.
- **Apply principle of least privilege**
  - Monitor for adversarial activities.
  - Hunt for brute force attempts.
  - Monitor for cleanup of Event Logs.
  - Analyze logon events.
- **Harden infrastructure**
  - Use Windows Defender Firewall.
  - Enable tamper protection.
  - Enable cloud-delivered protection.
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[56]

[56] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Mar. 10, 2025).

185. Since Defendant stored the PII of many individuals through the course of its business, Defendant could and should have implemented all of the above measures to prevent and detect the Data Breach that ultimately came to pass.

186. Specifically, among other failures, ABC Legal had vast amounts of unencrypted confidential information in its systems. Such PII should have been segregated and protected by an encrypted system.[57]

187. In sum, this Data Breach could have been prevented using industry standard network segmentation procedures and encrypting all confidential information. Further, the Data Breach could have been prevented if Defendant utilized appropriate malware prevention and detection technologies.

188. ABC Legal was negligent in its failure to ensure it had proper security measures in place to store Plaintiffs' and Class Members' confidential Private Information.

H. Defendant's Response to the Data Breach is Inadequate.

189. Defendant failed to timely inform Plaintiffs and Class Members of the Data Breach to adequately protect themselves from identity theft.

190. Defendant stated that the Data Breach was discovered in or around August 2024—months before Defendant notified Plaintiffs and the Class of the Breach. Defendant failed to inform Plaintiffs and Class Members exactly what information was exposed in the Data Breach and who carried out the Breach, leaving Plaintiffs and Class Members unsure as to the scope of information that was compromised and the dangers they faced.

191. If ABC Legal had investigated the Data Breach more diligently and reported it sooner, Plaintiffs and the Class could have taken steps to protect themselves and mitigate the harm suffered by the Breach.

[57] *See, e.g.*, Adnan Raja, *How to Safeguard Your Business Data with Encryption* (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption (last visited Mar. 10, 2025).

II. CLASS ACTION ALLEGATIONS

192. Plaintiffs incorporate by reference all preceding paragraphs as if fully restated herein.

193. Plaintiffs bring this action individually and on behalf of all members of the following class of similarly situated persons (collectively, the "Class" or "Class Member") against ABC Legal, pursuant to Federal Rule of Civil Procedure 23:

Nationwide Class

All persons residing in the United States who were sent a Notice Letter from ABC Legal.

Excluded from the Class is Defendant, any entity in which Defendant has a controlling interest, Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

194. In the alternative, Plaintiffs bring this action on behalf of themselves and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), and the following subclasses:

New York Subclass

All persons residing in the State of New York who were sent a Notice Letter from ABC Legal.

Oregon Subclass

All persons residing in the State of Oregon who were sent a Notice Letter from ABC Legal.

Excluded from the subclasses is Defendant, any entity in which Defendant has a controlling interest, Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

195. Plaintiffs reserve the right to amend the above definitions or to propose additional subclasses in subsequent pleadings and motions for class certification.

196. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

197. Numerosity: Upon knowledge and belief, there are at least 39,965 Members of the proposed Class and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendant's own records.

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

199. Adequacy of Representation: Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the other Class Members they seek to represent; Plaintiffs have retained counsel competent and highly experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

200. Superiority: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. No unusual difficulties are likely to be encountered in the management of this matter as a class action. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress ABC Legal's wrongdoing. Even if Class Members could afford such individual litigation, the Court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments and increase delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

201. Commonality and Predominance: Common questions of law and fact exist as to all proposed Class members and predominate over questions affecting only individual Class

Members. These common questions include:

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

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

c. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's PII;

d. Whether Defendant owed a legal duty to Plaintiffs and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII;

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

f. Whether Defendant failed to provide adequate cyber security;

g. Whether Defendant knew or should have known that its computer and network security systems were vulnerable to cyberattacks;

h. Whether Defendant's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its company network;

i. Whether Defendant was negligent in permitting unencrypted PII of vast numbers of individuals to be stored within its network;

j. Whether Defendant was negligent in permitting unencrypted PII of vast numbers of individuals to be stored within its network;

k. Whether Defendant was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees, applicants, and business associates;

l. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

m. Whether Defendant continues to breach duties to Plaintiffs and the Class;

n. Whether Plaintiffs and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

o. Whether Plaintiffs and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

p. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

III. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of all Plaintiffs and the Nationwide Class)

202. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

203. ABC Legal solicited, gathered, and stored the PII of Plaintiffs and the Class.

204. ABC Legal had full knowledge of the sensitivity of the PII it maintained and of the types of harm that Plaintiffs and Class Members could and would suffer if their PII were wrongfully disclosed. ABC Legal had a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiffs and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class Members had no ability to protect their PII that was in ABC Legal's possession. As such, a special relationship existed between ABC Legal and Plaintiffs and the Class.

205. ABC Legal was well aware of the fact that cybercriminals routinely target organizations in the legal services industry through cyberattacks in an attempt to steal the collected PII.

206. ABC Legal owed Plaintiffs and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing PII, including taking action to reasonably safeguard such

data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

207. ABC Legal's duties extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B.

208. ABC Legal had the duty to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to cyberattacks by encrypting documents containing PII, by not permitting documents containing unencrypted PII to be maintained on its systems, and other similarly common-sense precautions when dealing with sensitive PII. Additional duties that ABC Legal owed Plaintiffs and the Class include:

a) To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;

b) To protect the PII in its possession using reasonable and adequate security procedures and systems;

c) To adequately and properly audit and routinely test its systems;

d) To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

e) To adequately and properly audit, test, and train its employees regarding how to avoid phishing attempts and scams;

f) To train its employees not to store PII for longer than necessary;

g) To implement processes to quickly detect a data breach, security incident, or intrusion; and

h) To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

209. Plaintiffs and the Class were the intended beneficiaries of ABC Legal's duties, creating special relationships between them and ABC Legal. ABC Legal was in a position to ensure that its systems were sufficient to protect the PII that Plaintiffs and the Class had entrusted to it.

210. ABC Legal breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' PII. ABC Legal breached its duties by, among other things:

a) Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;

b) Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c) Failing to employ systems to protect against malware;

d) Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII, including maintaining it in an encrypted format;

e) Failing to adequately and properly audit, test, and train its employees regarding how to avoid phishing attempts and scams;

f) Failing to consistently enforce security policies aimed at protecting Plaintiffs and the Class's PII;

g) Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

h) Failing to abide by reasonable retention and destruction policies for PII it collects and stores; and

i) Failing to promptly and accurately notify Plaintiffs and Class Members of the Data Breach that affected their PII.

211. ABC Legal's willful failures to abide by these duties were wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

212. As a direct and proximate result of ABC Legal's grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

213. The damages Plaintiffs and the Class have suffered (as alleged above) were and are reasonably foreseeable.

214. The damages Plaintiffs and the Class have and will suffer were and are the direct and proximate result of ABC Legal's grossly negligent conduct.

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

216. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, ABC Legal prevented Plaintiffs and Class Members from taking meaningful, proactive steps toward securing their Private Information and mitigating damages.

217. As a result of the Data Breach, Plaintiffs and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to fraudulent activity, closely monitoring bank account activity, and examining credit reports and account statements. This is in addition to the identity theft and fraud Plaintiffs alleged.

218. ABC Legal's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

219. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of ABC Legal's grossly negligent conduct.

220. In addition to its duties under common law, ABC Legal had additional duties imposed by statute and regulations, including duties under the FTC Act. The harms which

occurred as a result of ABC Legal's failure to observe these duties, including the loss of privacy, lost time and expense, and significant risk of identity theft are the types of harm the FTC Act is intended to prevent.

221. ABC Legal violated the FTC Act when it engaged in the actions and omissions alleged herein, and Plaintiffs' and Class Members' injuries were a direct and proximate result of ABC Legal's violations of the FTC Act. Plaintiffs therefore are entitled to the evidentiary presumptions for negligence per se.

222. Pursuant to the FTC Act, 15 U.S.C. § 45(a), ABC Legal owed a duty to Plaintiffs and the Class to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and the Class.

223. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as ABC Legal, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also formed part of the basis of ABC Legal's duty in this regard.

224. ABC Legal gathered and stored the Private Information of Plaintiffs and the Class as part of its business, which affects commerce.

225. ABC Legal violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

226. ABC Legal breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class Members' Private Information, and by failing to provide prompt and specific notice without reasonable delay.

227. Plaintiffs and the Class are within the class of persons that the FTC Act is intended to protect.

228. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

229. ABC Legal breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's Private Information.

230. Additionally, ABC Legal had a duty to promptly notify victims of the Data Breach. ABC Legal did not begin notifying Plaintiffs or Class Members of the Data Breach until in or around December 2024. ABC Legal, however, knew of the Data Breach by August 2024.

231. ABC Legal breached its duties to Plaintiffs and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiffs and the Class.

232. As a direct and proximate result of ABC Legal's negligence, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

233. The injury and harm that Plaintiffs and Class Members suffered was the direct and proximate result of ABC Legal's negligence.

234. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

SECOND CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of all Plaintiffs and the Nationwide Class)

235. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

236. Plaintiffs allege this cause of action in the alternative or in addition to other causes of action where necessary.

237. Through the use of Plaintiffs' and Class Members' PII, Defendant received monetary benefits.

238. Defendant collected, maintained, and stored the PII of Plaintiffs and Class Members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon

it by Plaintiffs and Class Members.

239. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

240. However, acceptance of the benefit under the facts and circumstances described herein, make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, ABC Legal instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper and ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

241. Under the principle of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members because ABC Legal failed to implement the appropriate data management and security measures, and ABC Legal failed to ensure the appropriate data management and security measures were in place.

242. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

243. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to allow Defendant to have or maintain their PII.

244. As a direct and proximate result of ABC Legal's decision to profit rather than provide adequate data security, and as a direct and proximate cause of ABC Legal's failure to ensure it provided adequate data security, Plaintiffs and Class Members suffered and continue to suffer actual damages, including: (i) the amount of the savings and costs ABC Legal reasonably should have expended on data security measures to secure Plaintiffs' PII; (ii) time and expenses mitigating harms; (iii) diminished value of the PII; (iv) harms as a result of identity theft; and (v) an increased risk of future identity theft.

245. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiffs and the Class in direct violation of Plaintiffs' and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

246. Accordingly, Plaintiffs and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiffs and the Class.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of all Plaintiffs and the Nationwide Class)

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

248. Plaintiffs and Class Members were required to deliver their PII to Defendant as part of the process of obtaining employment and/or services provided by Defendant.

249. Defendant solicited, offered, and invited Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

250. Defendant accepted possession of Plaintiffs' and Class Members' PII for the purpose of providing employment and/or services to Plaintiffs and Class Members. Had Plaintiffs been aware that Defendant's network environment was not secure, they would not have entrusted Defendant with their PII.

251. Plaintiffs and the Class entrusted their PII to Defendant. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and

compromised or stolen.

252. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations (including the FTC guidelines on data security) and were consistent with industry standards.

253. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide PII, was the latter's obligation to: (i) use such PII for business purposes only; (ii) take reasonable steps to safeguard that PII; (iii) prevent unauthorized disclosures of the PII; (iv) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII; (v) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses; and (vi) retain the PII only under conditions that kept such information secure and confidential.

254. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

255. According to information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

256. According to information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' PII would remain protected.

257. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

258. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

259. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their email accounts, computer systems, and networks to ensure that it adopted reasonable data security measures.

260. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

261. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

262. Defendant breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their PII, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that their Private Information was compromised as a result of the Data Breach.

263. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate email accounts, computer systems, and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of PII and storage of other PII after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

264. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, 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 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and

adequate measures to protect the PII.

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

266. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant 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.

FOURTH CAUSE OF ACTION
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349
(On Behalf of Plaintiff Sanchez and the New York Subclass)

267. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

268. This Count is brought on behalf of Plaintiff Sanchez (hereinafter referred to as "Plaintiff" throughout this cause of action) and the New York Subclass (hereinafter referred to as "Class" throughout this cause of action).

269. New York General Business Law ("NYGBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

270. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of NYGBL § 349, and the deception occurred within New York State.

271. Defendant stored Plaintiff's and Class Members' Private Information in Defendant's electronic databases. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with all relevant regulations and would have kept Plaintiff's and Class Members' Private Information secure and prevented the loss or misuse of that Private Information. Defendant did not disclose to Plaintiff and Class Members that its data systems were not secure.

272. Plaintiff and Class Members would not have provided their Private Information if they had been told or knew that Defendant failed to maintain sufficient security thereof, and its inability to safely store Plaintiff's and Class Members' Private Information.

273. As alleged herein, Defendant engaged in the unfair or deceptive acts or practices in the conduct of consumer transactions in violation of N.Y. Gen. Bus. Law § 349, including but not limited to:

a) Representing that its services were of a particular standard or quality that it knew or should have known were of another;

b) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

c) Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

d) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

e) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' Private Information; and

274. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach.

275. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

276. Such acts by Defendant are and were deceptive acts or practices that are and/or were likely to mislead a reasonable consumer providing his or her Private Information to Defendant. Said deceptive acts and practices are material. The requests for and use of such Private Information in New York through deceptive means occurring in New York were consumer-oriented acts and thereby fell under the New York consumer fraud statute, NYGBL § 349.

277. In addition, Defendant's failure to secure its customers' Private Information violated the FTCA and therefore violates N.Y. Gen. Bus. Law § 349.

278. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Private Information of Plaintiff and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

279. The previously mentioned conduct violated N.Y. Gen. Bus. Law § 349, in that it is a restraint on trade or commerce.

280. Defendant's violations of N.Y. Gen. Bus. Law § 349 has an impact and general importance to the public, including the people of New York. Thousands of New Yorkers have had their Private Information stored on the ABC Legal's electronic database, many of whom have been impacted by the Data Breach.

281. In addition, New York residents have a strong interest in regulating the conduct of businesses within the legal industry, whose lax data security practices described herein have affected thousands of people across the country.

282. As a direct and proximate result of these deceptive trade practices, Plaintiff and Class Members are entitled to judgment under N.Y. Gen. Bus. Law § 349, to enjoin further violations, to recover actual damages, treble damages, and other monetary relief, to recover the

costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

FIFTH CAUSE OF ACTION
VIOLATIONS OF THE OREGON UNLAWFUL TRADE PRACTICE ACT
(On Behalf of Plaintiffs Rinne and Bodtker and the Oregon Subclass)

283. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

284. Plaintiffs Rinne and Bodtker (hereinafter referred to as "Plaintiffs" throughout this cause of action) on behalf of themselves and the the Oregon Subclass (hereinafter referred to as "Class" throughout this cause of action) are authorized to bring this claim under Or. Rev. Stat. § 646.638(1).

285. Or. Rev. Stat. § 646.608(1), et seq. ("OUTPA"), prohibits "unlawful practice[]s in the course of the person's business, vocation or occupation . . . ." Or. Rev. Stat. § 646.608(1).

286. As described in this Complaint, ABC Legal has engaged in the following unfair or deceptive acts or practices in violation of the OUTPA:

> (e) Represent[ing] that real estate, goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, quantities or qualities that the real estate, goods, or services do not have or that a person has a sponsorship, approval, status, qualification, affiliation, or connection that the person does not have;
>
> (g) Represent[ing] that real estate, goods or services are of a particular standard, quality, or grade, or that real estate or goods are of a particular style or model, if the real estate, goods or services are of another; and
>
> (u) Engag[ing] in any other unfair or deceptive conduct in trade or commerce.

Or. Rev. Stat. §§ 646.608(e), (g), (u).

287. ABC Legal's deceptive acts or practices in the conduct of commerce include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' Private Information, 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 Plaintiffs' and Class members' Private Information, 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 Plaintiffs' and Class members' Private Information, including implementing and maintaining reasonable security measures;

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

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Private Information;

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 Plaintiffs' and Class members' Private Information; and

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

288. ABC Legal is engaged in, and its acts and omissions affect trade and commerce. ABC Legal's relevant acts, practices, and omissions complained of in this action were done in the course of Defendant's business of marketing, offering for sale, and selling goods and services to consumers throughout the United States.

289. ABC Legal had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiffs' and Class members' Private Information. This exclusive knowledge includes, but is not limited to, information that ABC Legal received through internal and other non-public audits and reviews that concluded that ABC Legal's security policies were substandard and deficient, and that Plaintiffs' and Class members' Private Information and other ABC Legal data was vulnerable.

290. ABC Legal had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

291. ABC Legal also had exclusive knowledge about the length of time that it maintained individuals' Private Information after they stopped using services that necessitated the transfer of that Private Information to ABC Legal.

292. ABC Legal failed to disclose, and actively concealed, the material information it had regarding ABC Legal's deficient security policies and practices and regarding the security of the sensitive Private Information. For example, even though ABC Legal has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiffs' and Class members' Private Information was vulnerable as a result, ABC Legal failed to disclose this information to, and actively concealed this information from, Plaintiffs, Class members and the public. ABC Legal also did not disclose, and actively concealed, information regarding the extensive length of time that it maintains former customers' and employees' Private Information and other records.

293. Likewise, during the days and weeks following the Data Breach, ABC Legal failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

294. ABC Legal had a duty to disclose the material information that it had because, inter alia, it had exclusive knowledge of the information, it actively concealed the information, and because ABC Legal was in a fiduciary position by virtue of the fact that ABC Legal collected and maintained Plaintiffs' and Class members' Private Information.

295. ABC Legal's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of ABC Legal's data security and its ability to protect the confidentiality of current and former customers' and employees' Private Information.

296. Had ABC Legal disclosed to Plaintiffs and the Class that its data systems were not secure and, thus, vulnerable to attack, ABC Legal would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and Class members' Private Information without advising that ABC Legal's data security practices were insufficient to maintain the safety and confidentiality of their Private Information.

297. Accordingly, Plaintiffs and Class members acted reasonably in relying on ABC Legal's misrepresentations and omissions, the truth of which they could not have discovered.

298. ABC Legal'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.

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

300. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiffs and the Class as a direct result of ABC Legal's deceptive acts and practices as set forth herein include, without limitation: (i) Plaintiffs experiencing an increase in spam calls, texts, and/or emails; (ii) invasion of privacy; (iii) theft of their Private Information; (iv) lost or diminished value of Private Information; (v) lost time and opportunity costs associated

with attempting to mitigate the actual consequences of the Data Breach; (vi) loss of benefit of the bargain; (vii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in ABC Legal's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.The Data Breach was a direct result of ABC Legal's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its customers' and the employees' in its network Private Information from a foreseeable and preventable cyber-attack.

301. Plaintiffs 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 ABC Legal from disclosing their Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

SIXTH CAUSE OF ACTION
INVASION OF PRIVACY
(On Behalf of all Plaintiffs and the Nationwide Class)

302. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

303. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

304. Defendant owed a duty to its employees and customers, including Plaintiffs and the Class, to keep this information confidential.

305. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class Members' PII is highly offensive to a reasonable person.

306. The intrusion was into a place or thing which was private and entitled to be

private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant as part of their employment or for receiving Defendant's services, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

308. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

309. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

310. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

311. As a proximate result of Defendant's acts and omissions, the PII of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

312. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class because their PII are still maintained by Defendant with its inadequate cybersecurity system and policies.

313. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class.

314. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other

members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

SEVENTH CAUSE OF ACTION
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT, RCW 19.86
(On Behalf of Plaintiffs and the Putative Class)

315. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged herein.

316. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

317. Defendant is a "person" as described in RCW 19.86.010(1).

318. Defendant engages in "trade" and "commerce" as described in RCW 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the state of Washington.

319. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning of, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

320. Defendant's failure to safeguard the PII exposed in the Data Breach constitutes an unfair act that offends public policy.

321. Defendant's failure to safeguard the PII compromised in the Data Breach caused substantial injury to Plaintiffs and Class Members. Defendant's failure is not outweighed by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable by consumers.

322. Defendant's failure to safeguard the PII disclosed in the Data Breach, and its

failure to provide timely and complete notice of that Data Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

323. In the course of conducting its business, Defendant committed "unfair or deceptive 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 Plaintiffs' and Class Members' PII, and violating the common law alleged herein in the process. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

324. Defendant also violated the CPA by failing to timely notify, and by concealing from Plaintiffs and Class Members, information regarding the unauthorized release and disclosure of their PII. If Plaintiffs 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.

325. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

326. Defendant's unfair or deceptive acts or practices occurred in its trade or business and have injured and are capable of injuring a substantial portion of the public. Defendant's general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

327. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the CPA, Plaintiffs and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate, and continuing increased risk of identity theft and identity fraud—

risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) invasion of privacy; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (v) the financial and temporal costs of monitoring credit, monitoring financial accounts, and mitigating damages.

328. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves and the Class, seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant 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 the PII entrusted to it.

329. Plaintiffs, on behalf of herself and Class Members, also seek to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorneys' fees. In addition, Plaintiffs, on behalf of themselves and Class Members, request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained, not to exceed $25,000.00 per Class Member.

EIGHTH CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF
(On Behalf of all Plaintiffs and the Nationwide Class)

330. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

331. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

332. As previously alleged and pleaded, Defendant owed duties of care to Plaintiffs and Class Members that required it to adequately secure their PII.

333. Defendant still possesses the PII of Plaintiffs and the Class Members.

334. Defendant has not satisfied its obligations and legal duties to Plaintiffs and the Class Members.

335. ABC Legal has claimed that it is taking some steps to increase its data security, but there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Breach, and to once again place profits above protection.

336. Plaintiffs, therefore, seek a declaration (i) that ABC Legal's existing security measures do not comply with its obligations and duties of care to provide adequate security; and (ii) that to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

b) Order Defendant to significantly increase its spending on cybersecurity including systems and personnel;

c) Order Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;

d) Order Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

e) Order Defendant to segment Plaintiffs' and the Class's PII by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

f) Order Defendant to cease storing unencrypted PII on its systems;

g) Order Defendant to conduct regular database scanning and securing checks;

h) Order Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

i) Order Defendant to implement and enforce adequate retention policies for PII, including destroying, in a reasonably secure manner, PII once it is no longer necessary for it to be retained; and

j) Order Defendant to meaningfully educate its current, former, and prospective employees about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

IV. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all other similarly situated, pray for judgment against Defendant as follows:

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

b) An order finding that Defendant engaged in the unlawful conduct as alleged herein;

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

d) An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

e) An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

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

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

V. DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class, hereby demand a trial by jury on all appropriate issues raised in this Consolidated Class Action Complaint.

Date: March 10, 2025

/s/: Kaleigh N. Boyd
Kaleigh N. Boyd, WSBA #52684
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
Telephone: (206) 682-5600
E: kboyd@tousley.com

Raina Borrelli (admitted *pro hac vice*)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
E: raina@straussborrelli.com

Nickolas J. Hagman (admitted *pro hac vice*)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
E: nhagman@caffertyclobes.com

Kennedy M. Brian (admitted *pro hac vice*)
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120

Telephone: (405) 235-1560
Facsimile: (405) 239-2112
E: kpb@federmanlaw.com

Interim Co-Lead Class Counsel for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I, the undersigned, an attorney licensed to practice law in the State of Washington, certify that on March 10, 2025, I caused a true and correct copy of the attached Motion to be to all counsel of record via CM/ECF.

/s/: Kaleigh N. Boyd