Exhibit A

HONORABLE RICARDO S. MARTINEZ

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

BERNADETTE HIGHTOWER, LATERSHIA JONES, GEORGE DEAN, and BRUCE MARK WOODRUFF individually and on behalf of all others similarly situated, Plaintiffs, v. RECEIVABLES PERFORMANCE MANAGEMENT, LLC, Defendant.	Lead Case No. 2:22-cv-01683-RSM **AMENDED CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Bernadette Hightower, Latershia Jones, George Dean, and Bruce Mark Woodruff (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, and by and through their undersigned counsel, file this Consolidated Class Action Complaint against Defendant Receivables Performance Management, LLC ("RPM" or "Defendant") and allege the following based upon personal knowledge of the facts, and upon information and belief based on the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. Defendant provides debt collection services to various businesses, including telecommunications providers, utility providers, and financial institutions. To provide these

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

services and in the ordinary course of RPM's business, Defendant acquires, processes, analyzes, and otherwise utilizes the personally identifiable information of purported debtors, including, but not limited to, their names and Social Security numbers ("PII").

2. Defendant owed common law, contractual, and statutory duties to Plaintiffs and Class Members to design and implement adequate data security systems to protect the PII in its possession.

3. Moreover, by taking possession and control of Plaintiffs' and Class Members' PII, and utilizing the PII for its business purposes, Defendant assumed a duty to securely store and protect that sensitive information.

4. Defendant breached these duties by failing to properly safeguard and protect Plaintiffs' and Class Members' PII from a foreseeable cyberattack on its systems.

5. Specifically, on or about April 8, 2021, cybercriminals targeted, accessed, exfiltrated, and stole files on Defendant's network containing the PII of Plaintiffs and millions of other Class Members (the "Data Breach"). Defendant's monitoring practices were so poor that it did not identify this intrusion until May 12, 2021. Then, RPM reprehensibly waited until November 21, 2022—more than a year later—to begin notifying victims of the Data Breach.

6. Defendant has disclosed that in total, the Data Breach compromised the PII of approximately 3,766,573 people, including Plaintiffs' and Class Members' names and Social Security numbers.[1]

7. Defendant's negligent conduct—including, but not limited to, failing to implement adequate and reasonable data security measures to protect Plaintiffs' and Class Members' PII; failing to timely detect the Data Breach; failing to take adequate steps to prevent and stop the Data Breach; failing to disclose the material facts that it did not have adequate security practices and

[1] *See* Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/11ca5a7c-b09f-404a-81c6-b683305543a1.shtml (posting of data breach) (last visited Feb. 16, 2023).

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

employee training in place to safeguard the PII; failing to honor its promises and representations to protect Plaintiffs' and Class Members' PII; and failing to provide timely and adequate notice of the Data Breach—caused substantial harm and injuries to Plaintiffs and Class Members across the United States.

8. Furthermore, due to Defendant's negligence and data security failures, cybercriminals accessed, exfiltrated, and now likely possess, every type of PII they need to commit identity theft and wreak havoc on the financial and personal lives of millions of individuals.

9. As a result of the Data Breach, Plaintiffs and Class Members have suffered actual damages from the invasion of their privacy. Moreover, as a result of Plaintiffs' PII has been released to cybercriminals, Plaintiffs and Class Members are at an current and continuing, impending, and current risk of identity theft and fraud. This risk is realized and will continue for the rest of their lives, as Plaintiffs and Class Members are now forced to deal with the danger of identity thieves possessing and fraudulently using their PII.

10. In response to the Data Breach, Plaintiffs and Class Members lost time and money attempting to mitigate the impact of the Data Breach and following Defendant's warnings. Plaintiffs and Class Members anticipate spending additional time and money further mitigating the impact of the Data Breach, including but not limited to the cost of future identity theft monitoring services.

11. To be sure, the risk of harm is current, continuing, and concrete, as Plaintiff Hightower suffered actual fraudulent activity in her bank accounts, and Plaintiffs Jones and Dean both suffered a misuse of their data with the publication of their PII on the dark web. Other Class Members are believed to have experienced and suffered the same damages and losses throughout the country.

12. Plaintiffs brings this action individually and on behalf of the Class and seek past and future compensatory damages, nominal damages, statutory damages, treble damages, restitution, and injunctive and declaratory relief (including significant improvements to

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

Defendant's data security protocols and employee training practices), reasonable attorney's fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

THE PARTIES

13. Plaintiff Hightower is, and at all relevant times has been, a resident and citizen of the State of Pennsylvania.

14. Plaintiff Latershia Jones is, and at all relevant times has been, a citizen and resident of the Commonwealth of Virginia.

15. Plaintiff George Dean is, and at all relevant times has been, a resident and citizen of the State of Georgia.

16. Plaintiff Bruce Mark Woodruff is, and at all relevant times has been, a resident and citizen of the State of California.

17. Defendant is a Washington limited liability company with its principal place of business at 20818 44th Ave. W., Ste. 240, Lynnwood, WA 98036.

JURISDICTION AND VENUE

18. 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 Plaintiffs and members of the Class are citizens of states that differ from Defendant.

19. This Court has personal and general jurisdiction over Defendant because Defendant's principal place of business is located in this District, and Defendant conducts substantial business in Washington and this District through its principal place of business.

20. Venue is likewise proper as to Defendant in this District under 28 U.S.C. § 1391 because Defendant is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

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

FACTUAL ALLEGATIONS

A. The Data Breach

21. For RPM to perform its debt collection services, from which it generates its profits, Defendant collects and stores the PII of individuals, including Plaintiffs and the Class.

22. Due to the highly sensitive and personal nature of the information Defendant acquires and stores with respect to purported debtors, Defendant recognizes the privacy rights of the individuals whose PII Defendant obtains, as evidenced by RPM's publicly available privacy policy ("Privacy Notice").[2] Through its Privacy Notice, Defendant promises to maintain the privacy of individuals' PII and not disclose their PII without authorization. In particular, the Privacy Notice assures:

> We recognize and respect the privacy expectations of all people and make the safekeeping of all information a priority. . . . Our employees are educated on the importance of maintaining the confidentiality of information and of our privacy policy. In the event of a privacy breach by an employee, appropriate disciplinary action will be taken. ***We will maintain physical, electronic and procedural safeguards to guard against unauthorized access to information.***
>
> (emphasis added).

23. Plaintiffs and Class Members reasonably expected that Defendant would implement and maintain reasonable data security measures to protect their PII from foreseeable cybersecurity threats.

24. On or about May 12, 2021, Defendant became aware of a data security incident that impacted its server infrastructure and subsequently took Defendant's system offline. Defendant retained a forensic investigation firm that determined Defendant's systems were first accessed by cybercriminals on or about April 8, 2021. During this time, cybercriminals "accessed or acquired" Plaintiffs' and Class Members' PII, including their Social Security numbers. More than 3,700,000

[2] RPM, Receivables Performance Management, LLC, http://www.receivablesperformance.com/PrivacyPolicy.aspx (last visited Feb.16, 2023).

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

victims had their PII exposed as a result of the Data Breach.[3]

25. Based on Defendant's acknowledgement that PII was "acquired" by cybercriminals, it is evident that unauthorized cybercriminals did in fact access Defendant's files, and then exfiltrated and stole Plaintiffs' and Class Members' PII from those files.

26. On information and belief, Defendant failed to encrypt the PII contained in the files accessed by cybercriminals.

27. On information and belief, the cyberattack was targeted at Defendant due to its status as a major debt collector that obtains and stores large amounts of PII.

28. On information and belief, the targeted attack was expressly designed to gain access to and exfiltrate and steal private and confidential data, including the PII of Plaintiffs and the Class Members for criminal misuse, e.g., identity theft and financial fraud.

29. Moreover, while Defendant admits it learned of the Data Breach in May 2021, Defendant inexplicably waited ***one year and six months*** before it began the process of notifying impacted individuals, such as Plaintiffs and Class Members.

30. The fact that Defendant needed more than eighteen (18) months after learning of the Data Breach to investigate and begin notifying the impacted individuals of the need for them to protect themselves against fraud and identity theft only highlights the very poor state of Defendant's data security and tracking systems. Defendant was, of course, too late in the discovery, investigation, and notification of the Data Breach, which further left Plaintiff and Class Members' PII exposed.

31. Due to Defendant's inadequate security measures and its delayed notice to victims, Plaintiffs and the Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

[3] Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/11ca5a7c-b09f-404a-81c6-b683305543a1.shtml (posting of data breach) (last visited Feb. 16, 2023).

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

32. Defendant had duties and obligations created by industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their PII confidential and to protect that PII from unauthorized access and disclosure.

33. Plaintiffs and Class Members had the reasonable expectation that Defendant would comply with its duties and obligations to keep such information confidential and secure from unauthorized access and theft.

34. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

35. As a result of Defendant's negligent and wrongful conduct, Plaintiffs' and Class Members' sensitive PII was maintained in an inadequate and unsafe condition that allowed foreseeable criminal actors to access, exfiltrate, and steal their PII causing past, present, and future harms.

B. Plaintiffs' Experiences

Plaintiff Hightower's Experience

36. Plaintiff Hightower greatly values her privacy and is very careful with her PII. Plaintiff Hightower stores any documents containing PII in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Hightower has never knowingly transmitted sensitive PII over the internet in a manner that is unencrypted or unsecured. Moreover, Plaintiff Hightower diligently chooses unique usernames and passwords for her various online accounts. When Plaintiff Hightower does entrust a third-party with her PII, it is only because she understands such information will be reasonably safeguarded from foreseeable threats, and that she will be timely notified if her data is exposed.

37. Plaintiff Hightower provided PII, including her name, date of birth, and Social Security number, to her credit card company, one of Defendant's accounts receivable management

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

clients, as a condition of receiving financial services. Upon information and belief, Defendant thereafter acquired this PII and used this information when attempting to collect a purported debt.

38. Plaintiff Hightower received a letter dated November 21, 2022, from Defendant notifying her of the Data Breach. The letter advised that unauthorized third parties had accessed and exfiltrated files on Defendant's server containing Plaintiff Hightower's "personal information . . . including Social Security number . . . ."

39. Recognizing the present, immediate, and substantial risk of identity theft and fraud that Plaintiff Hightower now faces, Defendant offered Plaintiff Hightower a twelve-month subscription to credit monitoring services, which Defendant advised Plaintiff Hightower to enroll in so that she can "protect" herself "from potential harm associated with this incident . . . ." The letter further cautioned and warned Plaintiff Hightower to "remain vigilant for incidents of fraud and identity theft by reviewing account statements, explanation of benefit statements, and credit reports for unauthorized activity . . . ."

40. As a result of the Data Breach, Plaintiff Hightower heeded Defendant's warnings and advice and has spent approximately 30 hours researching the Data Breach, verifying the legitimacy of the notice letter, reviewing her bank accounts, monitoring her credit report, working with her financial institutions, filing a police report, changing her passwords and payment account numbers, and taking other necessary mitigation efforts. This is valuable time Plaintiff Hightower has spent at Defendant's direction and in response to the Data Breach that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

41. In addition, as a result of the Data Breach, Plaintiff Hightower suffered actual fraud with fraudulent activity on her Citizens Bank account in the early Summer of 2022 and more recently in October 2022. Specifically, Plaintiff Hightower noticed small amounts of money withdrawn from her bank account without her authorization.

42. Plaintiff Hightower would not have allowed her PII to be maintained by RPM had she known that Defendant would fail to safeguard that information from unauthorized access.

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

43. The Data Breach and fraudulent use of her PII also directly caused Plaintiff Hightower to suffer a loss of privacy.

44. As a result of the Data Breach, Plaintiff Hightower faces a substantial and current and continuing threat of identity theft and fraud that will exist for the rest of her life.

45. In response to the Data Breach and in heeding Defendant's warnings, Plaintiff Hightower has spent and anticipates spending additional time and money on an ongoing basis to try to mitigate and address the present and impending harm caused by the Data Breach.

46. The invasion of privacy and the substantial risk of identity theft and fraud have each caused Plaintiff Hightower to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

47. The Data Breach further caused Plaintiff Hightower to suffer a diminution in the value of her PII.

48. Plaintiff Hightower has a continuing interest in ensuring that her PII, which upon information and belief, remains in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Jones' Experience

49. Plaintiff Jones greatly values her privacy and is very careful with her PII. Plaintiff Jones stores any documents containing PII in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Jones has never knowingly transmitted sensitive PII over the internet in a manner that is unencrypted or unsecured. Moreover, Plaintiff Jones diligently chooses unique usernames and passwords for her various online accounts. When Plaintiff Jones does entrust a third-party with her PII, it is only because she understands such information will be reasonably safeguarded from foreseeable threats, and that she will be timely notified if her data is exposed.

50. Plaintiff Jones provided PII, including her name, date of birth, and Social Security number, to one of Defendant's clients as a condition of receiving services. Upon information and belief, Defendant thereafter acquired this PII and used this information when attempting to collect

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

a purported debt.

51. Plaintiff Jones received a letter dated November 21, 2022, from Defendant notifying her of the Data Breach. The letter indicated that unauthorized third parties accessed and exfiltrated files on Defendant's server containing Plaintiff Jones's "personal information . . . including Social Security number . . . ."

52. Recognizing the present, immediate, and substantial risk of identity theft and current and continuing financial harm that Plaintiff Jones now faces, Defendant offered Plaintiff Jones a twelve-month subscription to credit monitoring services, which Defendant encouraged Plaintiff Jones to enroll in so that she can "protect" herself "from potential harm associated with this incident . . . ." The letter further cautioned and warned Plaintiff Jones to "remain vigilant for incidents of fraud and identity theft by reviewing account statements, explanation of benefit statements, and credit reports for unauthorized activity …."

53. As a result of the Data Breach, Plaintiff Jones heeded Defendant's warning and has spent numerous hours researching the Data Breach, verifying the legitimacy of the notice letter, placing freezes on her credit, reviewing her bank accounts, monitoring her credit reports, monitoring her other information, changing her passwords and other identifying information, and taking other necessary mitigation efforts. This is valuable time Plaintiff Jones spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

54. In addition, Plaintiff Jones has already experienced data misuse as a result of the Data Breach. Specifically, in the months following the Data Breach, Plaintiff Jones received notification that her Social Security number was compromised and found on the dark web.

55. Plaintiff Jones would not have allowed her PII to be maintained by RPM had she known that Defendant would fail to safeguard that information from unauthorized access.

56. The Data Breach and publication of her information on the Dark Web has caused Plaintiff Jones to suffer a loss of privacy.

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

57. As a result of the Data Breach, Plaintiff Jones faces a substantial, current, and continuing, and imminent threat of identity theft and fraud that she will face for the remainder of her life.

58. Plaintiff Jones has spent time and anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

59. The invasion of privacy and substantial risk of identity theft and fraud have each caused Plaintiff Jones to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

60. The Data Breach caused Plaintiff Jones to suffer a diminution in the value of her PII.

61. Plaintiff Jones has a continuing interest in ensuring that her PII, which upon information and belief, remains in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Dean's Experience

62. Plaintiff Dean greatly values his privacy and is very careful with his PII. Plaintiff Dean stores any documents containing PII in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Dean has never knowingly transmitted sensitive PII over the internet in any manner that is unencrypted or unsecured. Moreover, Plaintiff Dean diligently chooses unique usernames and passwords for his online accounts. When Plaintiff Dean does entrust a third-party with his PII, it is only because he understands such information will be reasonably safeguarded from foreseeable threats, and that he will be timely notified if his data is exposed.

63. Plaintiff Dean provided PII, including his name, date of birth, and Social Security number, to one of Defendant's clients as a condition of receiving services. Upon information and belief, Defendant thereafter acquired this PII and used this information when attempting to collect a purported debt.

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

64. Plaintiff Dean received a letter dated November 21, 2022, from Defendant notifying him of the Data Breach. The letter advised that unauthorized third parties accessed and exfiltrated files on Defendant's server containing Plaintiff Dean's "personal information . . . including Social Security number . . . ."

65. Recognizing the present, immediate, and substantial risk of identity theft, current, and continuing financial harm Plaintiff Dean faces, Defendant offered Plaintiff Dean a twelve-month subscription to credit monitoring services, which Defendant encouraged Plaintiff Dean to enroll in so that he can "protect" himself "from potential harm associated with this incident . . . ." The letter, however, did not include any instructions on how to enroll in the service.

66. Defendant further cautioned and warned Plaintiff Dean to "remain vigilant for incidents of fraud and identity theft by reviewing account statements, explanation of benefits statements, and credit reports for unauthorized activity . . . ."

67. Additionally, on January 25, 2023, Plaintiff Dean received a notification from IDNotify that his personal information was found on the Dark Web.

68. As a result of the Data Breach, and in heeding Defendant's warnings, Plaintiff Dean spent more than five (5) hours researching the Data Breach, verifying the legitimacy of the notice letter, reviewing his bank accounts, monitoring his credit report, changing passwords, and other necessary mitigation efforts. This is valuable time Plaintiff Dean spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

69. Plaintiff Dean would not have allowed his PII to be maintained by RPM had he known that Defendant would fail to safeguard that information from unauthorized access.

70. The Data Breach and subsequent publication of his PII on the dark web caused Plaintiff Dean to suffer a loss of privacy.

71. As a result of the Data Breach, Plaintiff Dean now faces a substantial risk of identity theft and current and continuing financial harm for the remainder of his life.

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

72. Plaintiff Dean has spent considerable time and anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending harm caused by the Data Breach.

73. The invasion of privacy and substantial risk of identity theft and fraud have each caused Plaintiff Dean to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

74. The Data Breach caused Plaintiff Dean to suffer a diminution in the value of his PII.

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

Plaintiff Woodruff's Experience

76. Plaintiff Woodruff greatly values his privacy and is very careful with his PII. Plaintiff Woodruff stores any documents containing PII in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Woodruff has never knowingly transmitted sensitive PII over the internet in a manner that is unencrypted or unsecured. Moreover, Plaintiff Woodruff diligently chooses unique usernames and passwords for his various online accounts. When Plaintiff Woodruff does entrust a third-party with his PII, it is only because he understands such information will be reasonably safeguarded from foreseeable threats, and that he will be timely notified if his data is exposed.

77. Plaintiff Woodruff provided PII, including his name, date of birth, and Social Security number, to one of Defendant's clients as a condition of receiving services. Upon information and belief, Defendant thereafter acquired this PII and used this information when attempting to collect a purported debt.

78. Plaintiff Woodruff received a letter dated November 21, 2022, from Defendant notifying him of the Data Breach. The letter indicated that unauthorized third parties accessed and exfiltrated files on Defendant's server containing Plaintiff Woodruff's "personal information . . .

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

including Social Security number . . . ."

79. Recognizing the present, immediate, and substantial risk of identity theft and current and continuing financial harm that Plaintiff Woodruff now faces, Defendant offered Plaintiff Woodruff a twelve-month subscription to credit monitoring services, which Defendant encouraged Plaintiff Woodruff to enroll in so that he can "protect" himself "from potential harm associated with this incident . . . ." The letter further cautioned and warned Plaintiff Woodruff to "remain vigilant for incidents of fraud and identity theft by reviewing account statements, explanation of benefit statements, and credit reports for unauthorized activity . . . ."

80. As a result of the Data Breach, Plaintiff Woodruff heeded Defendant's warning and has spent numerous hours researching the Data Breach, verifying the legitimacy of the notice letter, placing freezes on his credit, reviewing his bank accounts, monitoring his credit reports, monitoring his other information, changing his passwords and other identifying information, and taking other necessary mitigation efforts. This is valuable time Plaintiff Woodruff spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

81. Plaintiff Woodruff would not have allowed his PII to be maintained by Defendant had he known that Defendant would fail to safeguard that information from unauthorized access.

82. As a result of the Data Breach, Plaintiff Woodruff faces a substantial and current and continuing threat of identity theft and fraud that he will face for the remainder of his life.

83. Plaintiff Woodruff has spent time and anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

84. The invasion of privacy and substantial risk of identity theft and fraud have each caused Plaintiff Woodruff to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

85. The Data Breach caused Plaintiff Woodruff to suffer a diminution in the value of his PII.

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

86. Plaintiff Woodruff has a continuing interest in ensuring that his PII, which upon information and belief, remains in Defendant's possession, is protected, and safeguarded from future breaches.

C. Defendant Was on Notice of Data Threats in the Industry and of the Inadequacy of Its Data Security

87. Defendant was on notice that companies, such as Defendant, maintaining large amounts of PII during their regular course of business, are prime targets for criminals looking to gain unauthorized access to sensitive and valuable information, such as the type of data at issue in this matter.

88. At all relevant times, RPM knew, or should have known, that the PII that it collected was a target for malicious actors. Despite such knowledge, and well-publicized cyberattacks on similar companies, RPM failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' PII from cyber-attacks that RPM should have anticipated and guarded against.

89. It is well known among companies that store sensitive PII that sensitive information—such as the Social Security numbers stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[4]

90. In light of recent high profile data breaches, including Microsoft (250 million records, December 2019), T-Mobile (110 million records, August 2021), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion

[4] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last visited Feb. 16, 2023).

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

records, May 2020), RPM knew or should have known that its electronic records would be targeted by cybercriminals.

91. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, take appropriate measures to prepare for, and are able to thwart such an attack.

92. Moreover, PII is a valuable property right.[5] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[6] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[7] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" or the "dark web" for many years.

93. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

94. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is

---

[5] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[6] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, No. 220, Apr. 2, 2013, https://doi.org/10.1787/5k486qtxldmq-en.

[7] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

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

considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[8]

95. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

D. Cyber Criminals Will Use Plaintiffs' and Class Members' PII to Defraud Them

96. Plaintiffs' and Class Members' PII is of great value to cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

97. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[9] For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, 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 to police during arrests, and many other harmful forms of identity theft.[10] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

98. PII is such a valuable commodity to identity thieves that once it has been

---

[8] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RES. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[9] "Facts + Statistics: Identity Theft and Cybercrime," INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last accessed Feb. 16, 2023).

[10] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number?*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited Feb. 16, 2023).

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

compromised, criminals will use it and trade the information on the cyber black-market for years.[11]

99. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.[12]

100. The PII exposed the Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[13]

101. Cyber criminals may not use the information right away. 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.[14]

102. For instance, with a stolen Social Security number, which is only one category of the PII compromised in the Data Breach, someone can open financial accounts, file fraudulent tax returns, commit crimes, and steal benefits.[15]

---

[11] United States Government Accountability Office, Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

[12] *See* Jon Fingas, *Fraud Ring Uses Stolen Data to Scam Unemployment Insurance Programs*, ENGADGET (May 17, 2020, 1:46 PM), https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html (last accessed Feb. 16, 2023); *see also* Lily H. Newman, *The Nigerian Fraudsters Ripping Off the Unemployment System*, WIRED (May 19, 2020, 7:00 AM), https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/ (last visited Feb. 16, 2023).

[13] Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info (last accessed Feb. 16, 2023).

[14] *Data Breaches Are Frequent*, *supra* note 11.

[15] *See, e.g.*, *What Can You Do with a Stolen Social Security Number?*, *supra* note 10.

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

103. Victims of the Data Breach, like Plaintiffs and other Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[16]

104. In fact, as a direct and proximate result of the Data Breach, Plaintiffs and the Class have been placed at an current, continuing, immediate, and continuing risk of harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and other information for unauthorized activity for years to come.

105. Plaintiffs and the Class have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

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

b. Improper disclosure of their PII;

c. The current, continuing, and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;

d. The current, continuing, and certainly impending risk of having their confidential information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

[16] Identity Theft – A Recovery Plan, FED. TRADE COMM'N, (Sept. 2018), https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf (last visited Feb. 16, 2016); *see also* Identity Theft – What to Know, What to Do, FED. TRADE COMM'N (Sept. 2018), https://www.bulkorder.ftc.gov/system/files/publications/677a_idt_what_to_know_wtd.pdf.

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

f. Loss of privacy suffered as a result of the Data Breach;

g. 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;

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

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

j. Damage to their credit due to fraudulent use of their PII; and

k. Increased cost of borrowing, insurance, deposits, and other items, which are adversely affected by a reduced credit score.

106. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily-compliant security measures and safeguards. Defendant has shown itself to be wholly incapable of protecting Plaintiffs' and Class Members' PII.

107. Plaintiffs and Class Members have been taking and will continue to take appropriate steps to mitigate the risk of harm and damage that Defendant has caused them but, given the kind of PII Defendant made so easily accessible to cyber criminals, they are certain to incur additional damages. Because identity thieves already have their PII, Plaintiffs and 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 arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[17]

[17] *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 Feb. 16, 2023).

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

108. To be sure, Plaintiffs should not be in the current compromised position with respect to their identities and financial affairs, and Plaintiffs should not have been forced to take time consuming and expensive mitigation measures to protect themselves from identity theft and fraud. None of this should have happened because the Data Breach was entirely preventable.

E. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiffs' and Class Members' PII

109. Data disclosures and data breaches are preventable.[18] 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."[19] 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 . . . ."[20]

110. "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*."[21]

111. Defendant obtained and stored Plaintiffs' and Class Members' PII—including, but not limited to, their names Social Security numbers—and was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such PII.

112. Defendant breached duties owed to Plaintiffs and the Class as guardian of their PII.

113. Many failures laid the groundwork for the occurrence of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber

---

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

[19] *Id.* at 17.

[20] *Id.* at 28.

[21] *Id.*

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

security training, procedures, and protocols that were necessary to protect Plaintiffs' and Class Members' PII.

114. Defendant maintained the PII in an objectively reckless manner, making the PII vulnerable to unauthorized disclosure.

115. Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if Plaintiffs' and Class Members' PII was stolen, including the significant costs that would be placed on Plaintiffs and Class Members as a result of a breach.

116. The risk of improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiffs' and Class Members' PII from that risk left the PII in a dangerous condition.

117. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the PII was protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

i. Defendant Could Have Prevented the Data Breach by Implementing Widely Distributed Expert-Recommended Measures

118. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time or for whom there was no reasonably anticipated future use.

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

119. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

120. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members.

121. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[22]

122. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

123. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

[22] *See generally* https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last accessed October 21, 2022).

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

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

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

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[23]

124. To prevent and detect cyberattacks, including the cyberattack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

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

- Use caution with links and when entering website addresses. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or 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.

[23] How to Protect Your Networks from RANSOMWARE, at 3–4, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Feb. 22, 2023).

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

- 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 . . . .[24]

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

- Secure internet-facing assets
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials
- Thoroughly investigate and remediate alerts
  - Prioritize and treat commodity malware infections as potential full compromise;
- Include IT Pros in security discussions
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely
- Build credential hygiene

[24] *See Security Tip* (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Feb. 22, 2023).

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

- 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].[25]

126. Moreover, given that Defendant was storing PII of Plaintiffs and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

127. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of Plaintiff and Class Members.

128. As a result of computer systems in need of security upgrades, as well as inadequate procedures for handling email phishing attacks, viruses, malignant computer code, and hacking

[25] *See Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed Feb. 22, 2023).

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

attacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII.

129. Because Defendant failed to properly protect and safeguard Plaintiffs' and Class Members' PII, an unauthorized third party was able to access Defendant's network and access Defendant's database and system configuration files and exfiltrate that data.

ii. Defendant Failed to Comply with FTC Guidelines

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

131. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[26]

132. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

133. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity

[26] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (2016), *available at* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

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

on the network; and verify that third-party service providers have implemented reasonable security measures.

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

135. Defendant failed to properly implement basic data security practices.

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

137. Defendant was always fully aware of its obligation to protect the PII of Plaintiff and Class Members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

iii. Defendant Failed to Comply with Industry Standards

138. As shown above, experts studying cyber security routinely identify entities like RPM as being particularly vulnerable to cyberattacks because of the value of the PII that they collect and maintain.

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

140. Other best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email

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

management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

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

142. The foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

143. Upon information and belief, Defendant failed to comply with one or more of the foregoing industry standards.

COMMON INJURIES & DAMAGES

144. As result of Defendant's ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing current and continuing risk of fraud and identity theft.

145. Due to the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is current and continuing, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and current and continuing threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and current and continuing threat of identity theft; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g)

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

the loss of benefit of the bargain (price premium damages); (h) diminution of value of their PII; and (i) the continued risk to their PII, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

A. The Risk of Identity Theft and Fraud to Plaintiffs and Class Members Is Present and Ongoing

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

147. Because a person's identity is akin to a puzzle with multiple data points, the greater the number of accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity directly, or to track the victim to attempt other hacking crimes that will allow them to obtain more data to perfect a crime.

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

149. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[27] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web

[27] *What Is the Dark Web?*, EXPERIAN (May 12, 2021), *available at* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

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

users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[28] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

150. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.[29] The digital character of PII stolen in data breaches, specifically this Data Breach, lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs, on the other hand, requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[30] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[31]

151. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being

---

[28] *Id.*

[29] *What is the Dark Web?*, MICROSOFT 365 (July 15, 2022), *available at* https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

[30] *Id.*; *What Is the Dark Web?*, EXPERIAN (May 12, 2021), *available at* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[31] *What is the Dark Web?*, MICROSOFT 365 (July 15, 2022), *available at* https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

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

issued in the victim's name. The Social Security Administration has warned that identity thieves can also use an individual's Social Security number to apply for additional credit lines.[32]

152. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[33]

153. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[34] Defendant did not rapidly report to Plaintiffs and the Class that their PII had been stolen.

154. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

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

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

---

[32] *Identity Theft and Your Social Security Number*, SOC. SEC. ADMIN. (2018) at 1, *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Feb. 22, 2023).

[33] *See 2019 Internet Crime Report Released* (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last accessed Feb. 22, 2023).

[34] *Id.*

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

157. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[35]

158. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[36]

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

B. Loss of Time to Mitigate the Risk of Identify Theft and Fraud

160. As a result of the recognized risk of identity theft, when a Data Breach occurs and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn

---

[35] Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited Feb. 22, 2023).

[36] *See generally Protecting Personal Information*, *supra* note 26.

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

about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the resource and asset of time has been lost.

161. Thus, due to the actual and current and continuing risk of identity theft, Plaintiffs and Class Members must, as Defendant's Data Breach Notice instructs them to do, "closely monitor all mail, email, and other contact from individuals not known to you personally" and to "remain vigilant for fraud or identity theft by reviewing account statements, explanation of benefits statements, and credit reports for unauthorized activity . . . ."

162. Plaintiffs and Class Members have spent time, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing, or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports.

163. Plaintiffs' mitigation efforts are consistent with guidance from the U.S. Government Accountability Office, which released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[37]

164. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a

[37] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* GAO-07-737, U.S. GOV'T ACCOUNTABILITY OFFICE, (June 2007), https://www.gao.gov/new.items/d07737.pdf.

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

credit freeze on their credit, and correcting their credit reports.[38]

C. Diminution of Value of the PII

165. PII is a valuable property right.[39] Considering the value of Big Data in corporate America, and the potential consequences to cyber thieves (including heavy prison sentences), its value is axiomatic. Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

166. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[40]

167. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[41] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker, who in turn aggregates the information and provides it to marketers or app developers.[42] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[43]

168. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and black markets, has been damaged and diminished by

---

[38] *See* FED. TRADE COMM'N, IDENTITY THEFT.GOV, https://www.identitytheft.gov/Steps (last visited Feb. 22, 2023).

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

[40] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Feb. 22, 2023).

[41] David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak* (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[42] *See, e.g.*, https://datacoup.com/; https://worlddataexchange.com/about.

[43] Computer & Mobile Panel, NIELSEN, *available at* https://computermobilepanel.nielsen.com/ui/US/en/sdp/landing (last visited Feb. 22, 2023).

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

its unauthorized release onto the Dark Web, where it is now available and holds significant value for the threat actors. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of Plaintiffs' and Class Members' PII has been lost, thereby causing additional loss of value.

D. Future Cost of Credit and Identify Theft Monitoring Is Reasonable and Necessary

169. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach—Defendant has offered only 12 months of inadequate identity monitoring services, despite Plaintiffs and Class Members being at risk of identity theft and fraud for the foreseeable future. Defendant has not offered any other relief or protection.

170. The 12 months of credit monitoring offered to persons whose PII was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. Defendant also places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

171. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, reports of misuse of Plaintiffs' PII discussed above, and reports of dissemination on the Dark Web also discussed above, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes, including opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

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

172. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

173. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[44] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

174. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

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

E. Injunctive Relief Is Necessary to Protect Against Future Data Breaches

176. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

---

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

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

CLASS ACTION ALLEGATIONS

177. Plaintiffs bring this action under Federal Rule of Civil Procedure 23 against Defendant individually and on behalf of all others similarly situated. Plaintiffs assert all claims on behalf of the Class, defined as follows:

> **Nationwide Class**
> All persons residing in the United States whose personally identifiable information was accessed or acquired as a result of the Data Breach that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and other Class Members on or around November 21, 2022 (the "Nationwide Class").

178. Plaintiffs also seek to represent the following state subclass defined as:

> **Georgia Subclass**
>
> All Georgia residents whose personally identifiable information was accessed or acquired as a result of the Data Breach that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and other Class Members on or around November 21, 2022 (the "Georgia Subclass").

179. Plaintiff also seeks to represent the following state subclass defined as:

> **California Subclass**
>
> All California residents whose personally identifiable information was accessed or acquired as a result of the Data Breach that is the subject of the Notice of Data Breach that Defendant sent to Plaintiff and other Class Members on or around November 21, 2022 (the "California Subclass").

180. The Nationwide Class and the state Subclasses are referred to collectively as the Class. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

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

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

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

183. Numerosity: The proposed Class is believed to be so numerous that joinder of all members is impracticable. Indeed, Defendant has disclosed that in total, the Data Breach compromised the PII of approximately 3,766,573 people, including Plaintiffs and Class Members.[45]

184. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class Member because Plaintiffs and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Defendant.

185. Adequacy: Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class they seek to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and Plaintiffs' counsel.

186. Superiority: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. 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 to individually and effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation

[45] *See* Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/11ca5a7c-b09f-404a-81c6-b683305543a1.shtml (last visited Feb. 16, 2023).

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

presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

187. Commonality and Predominance: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

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

b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class Members' PII;

c. Whether Defendant's computer systems and data security practices used to protect Plaintiffs' and Class Members' PII violated the FTC Act, and/or state laws and/or Defendant' other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their PII, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems were vulnerable to a data breach or disclosure;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties to Plaintiffs and the Class to use reasonable care in protecting their PII;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals

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

in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

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

j. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief;

k. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the current, continuing, and currently ongoing harm faced by Plaintiffs and members of the Class; and

l. Whether Plaintiffs and Class Members are entitled to treble damages.

CAUSES OF ACTION

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

188. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

189. Defendant gathered and stored the PII of Plaintiffs and the Class as part of the operation of its business and benefited from holding and using the PII in its business operations.

190. Upon accepting, storing, and utilizing the PII of Plaintiffs and Class Members for its benefit, Defendant undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods and to implement necessary data security protocols and employee training to do so.

191. Defendant had full knowledge of the sensitivity of the PII, the types of harm that Plaintiffs and Class Members could and would suffer if the PII was wrongfully disclosed, the importance of adequate data security, and of prior data breaches.

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

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

193. Defendant owed Plaintiffs and 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 their 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.

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

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

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

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

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

c. To promptly notify Plaintiffs and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their PII.

196. Defendant also had a duty to protect Plaintiffs' and the Class's PII because Defendant engaged in an affirmative act or misfeasance such that it increased the risk of financial harm to the Plaintiffs and otherwise created a situation of peril for Plaintiffs and the Class. Defendant knowingly and deliberately chose not to employ adequate data security to save on costs, despite being on notice of rampant data breaches across the country. These negligent acts placed Plaintiffs and Class Members at an current and continuing risk of identity theft and fraud and created a situation of peril for Plaintiffs and the Class by leaving their PII vulnerable to exposure and theft by criminal actors.

197. Only Defendant was in a position to ensure that its data systems and protocols were sufficient to protect the PII that had been entrusted to it.

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

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting 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 adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

d. Failing to adequately train its employees to not store unencrypted PII in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

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

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

f. Failing to mitigate the harm caused to Plaintiffs and the Class Members;

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

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

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

200. As a proximate and foreseeable result of Defendant's negligent conduct, Plaintiffs and the Class have suffered damages and are at a current and continuing risk of identity theft, fraud, and additional harms and damages (as alleged above).

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

202. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII and mitigate damages.

203. As a result of the Data Breach and subsequent notification letters, 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 the fraudulent use of their PII and closely reviewing and monitoring bank accounts, credit reports, and financial statements.

204. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence and recklessness.

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

205. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent and reckless conduct.

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

SECOND CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

207. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

208. Defendant entered into various written contracts with its clients to perform services that include, but are not limited to, debt recovery services.

209. These contracts were made in part for the benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. The contracts were made with the intent and expectation that Plaintiffs' and Class Members' PII would remain private and would be adequately protected from unauthorized disclosure. Indeed, Defendant knew that if it were to breach these contracts with its clients, the clients' customers—Plaintiffs and Class Members—would be harmed.

210. It was intended by Defendant and its clients at the time the contracts were made that Defendant would assume a direct obligation to protect Plaintiffs' and the Class's PII.

211. It was also intended by Defendant and its clients that the performance under the contract would necessarily and directly benefit Plaintiffs and the Class. Defendant would collect payment from Plaintiffs and the Class and Defendant would expunge their debt in return.

212. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures and (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' PII from unauthorized disclosure to third parties.

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

213. As foreseen, Plaintiffs and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to compensatory damages they have sustained as a direct and proximate result thereof.

THIRD CAUSE OF ACTION
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT (RCW 19.86.010 *ET SEQ.*)
(On Behalf of the Nationwide Class)

214. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

215. 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. The CPA does not define "unfair" or "deceptive."

216. Either an unfair or a deceptive act or practice may serve as the basis of a CPA claim. *See Veridian Credit Union v. Eddie Bauer, LLC*, 295 F. Supp. 3d 1140, 1161 (W.D. Wash. 2017) (citation omitted).

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

218. 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.

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

220. In the course of conducting its business, Defendant committed "unfair acts or practices" by, among other things, 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

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

Class Members' PII. Plaintiffs and the Class reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's unfair acts and practices are ongoing and continue to this date.

221. These unfair acts have caused substantial injury to Plaintiffs and the Class because their PII has been exposed to cyber criminals who will commit identity theft and fraud. Plaintiffs and the Class were unable to avoid Defendant servicing their accounts because Defendant was selected by its clients. Further, Defendant's unfair acts have no countervailing benefits; Plaintiffs and the Class will not benefit from the exposure of their PII.

222. Defendant's conduct was also deceptive. Defendant concealed from Plaintiffs and Class Members the unauthorized release and disclosure of their PII, and it failed to timely notify them of that unauthorized release and disclosure. 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.

223. Defendant's above-described "unfair or deceptive acts or practices" affects the public interest because it is substantially injurious to persons and has the capacity to injure other persons.

224. 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.

225. Defendant's above-described unfair and deceptive acts and practices directly and proximately caused injury to Plaintiffs' and Class Members' business and property. Plaintiffs and Class Members have suffered, and will continue to suffer, actual damages and injury in the form of, among other things, (1) a current, continuing, , immediate, and continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which Plaintiffs and Class Members are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of Plaintiffs' and Class Members' PII; (5) deprivation of the value of

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

Plaintiffs' and Class Members' PII, for which there is a well-established national and international market; (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages; and/or (7) investment of substantial time and money to monitoring and remediating the harm inflicted upon them.

226. 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, Class Members, and the general public, also seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct and requiring Defendant to modify its corporate culture and 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.

227. Plaintiffs 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.

228. In addition, Plaintiffs, on behalf of themselves and the 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.

FOURTH CAUSE OF ACTION
VIOLATIONS OF THE GEORGIA SECURITY BREACH NOTIFICATION ACT, O.C.G.A. § 10-1-912, *ET SEQ.*
(On behalf of Plaintiff Dean and the Georgia Subclass)

229. Plaintiff Dean ("Plaintiff," for purposes of this Count) incorporates by reference the foregoing paragraphs as if fully set forth herein.

230. Plaintiff brings this count on behalf of the Georgia Subclass.

231. Defendant is a business that owns or licenses computerized data that includes PII as defined by O.C.G.A. § 10-1-912(a).

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

232. Plaintiff and Georgia Subclass Members' PII that was compromised in the Data Breach includes PII covered under O.C.G.A. § 10-1-912(a).

233. Defendant is required to accurately notify Plaintiff and Georgia Subclass Members if it becomes aware of a breach of its data security systems that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Georgia Subclass Members' PII in the most expedient time possible and without unreasonable delay under O.C.G.A. § 10-1-912(a).

234. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated O.C.G.A. § 10-1-912(a).

235. As a direct and proximate result of Defendants' violations of O.C.G.A. § 10-1-912(a), Plaintiff and Georgia Subclass members suffered damages, as described above.

236. Plaintiff and Georgia Subclass members seek relief under O.C.G.A. § 10-1-912, including actual damages and injunctive relief.

FIFTH CAUSE OF ACTION
VIOLATIONS OF THE GEORGIA DECEPTIVE PRACTICES ACT,
GA. CODE ANN. §§ 10-1-370, *ET SEQ.*
(On behalf of Plaintiff Dean and the Georgia Subclass)

237. Plaintiff Dean ("Plaintiff," for purposes of this Count) and the Georgia Subclass incorporate by reference the foregoing paragraphs as if fully set forth herein.

238. RPM, Plaintiff, and the Georgia Subclass members are "persons" within the meaning of the Georgia Deceptive Trade Practices Act ("Georgia DTPA"), Ga. Code Ann. § 10-1-370(5).

239. The Georgia DTPA states the following at Ga. Code Ann. § 10-1-372:

> (a) A person engages in a deceptive trade practice when, in the course of his business, vocation, or occupation, he: . . . (5) Represents that goods or services have . . . characteristics, . . . uses, [or] benefits . . . that they do not have; . . . (7) Represents that goods or services are of a particular standard, quality, or grade . . . if they are of another; . . . [or] (12) Engages in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.

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

240. RPM engaged in deceptive trade practices in violation of Ga. Code Ann. § 10-1-372(a)(5), (7), and (12) by, among other things:

(a) Omitting and concealing the material fact that it did not employ reasonable measures to secure consumers' PII. RPM could and should have made a proper disclosure to consumers (including its clients and Georgia Subclass Members), during its engagement process or debt collection process, or by any other means reasonably calculated to inform consumers of the inadequate data security; and

(b) Making implied or implicit representations that its data security practices were sufficient to protect consumers' PII. RPM acquired consumers' PII during the debt collection process. In doing so, RPM made implied or implicit representations that its data security practices were sufficient to protect consumers' PII. By virtue of accepting Plaintiffs' PII during the collection process, RPM implicitly represented (including to RPM's clients who may not have elected to use RPM for their collections had they known the true state of affairs) that its data security processes were sufficient to safeguard the PII.

241. The Georgia DTPA states that "[i]n order to prevail in an action under this part, a complainant need not prove . . . actual confusion or misunderstanding." Ga. Code Ann. § 10-1-372(b).

242. The Georgia DTPA further states: "A person likely to be damaged by a deceptive trade practice of another may be granted an injunction against it under the principles of equity and on terms that the court considers reasonable. Proof of monetary damage, loss of profits, or intent to deceive is not required." Ga. Code Ann. § 10-1-373(a).

243. While Defendant provided notice of the Date Breach, Defendant has not provided sufficient details regarding the full scope of the Data Breach or any details related to the remedial measures that it has taken to improve and more fully safeguard Plaintiffs' and Georgia Subclass Members' data from future compromise. As a result, Plaintiffs, Georgia Subclass Members, and RPM's clients remain uninformed and confused as to the adequacy of RPM's data security and

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

RPM's ability to protect the PII entrusted to it. Without adequate improvements, Plaintiffs' and Georgia Subclass' Members data remains at an unreasonable risk for future compromise.

244. Moreover, Defendant, through its omissions and Notice Letter, continues to represent and imply that its data security measures are adequate to protect the PII of Plaintiff and the Georgia Subclass. Such continued representations and implications, without disclosure of the full scope of the Data Breach or remedial enhancements, place Plaintiffs and Georgia Subclass Members at a future risk of harm, as Plaintiffs, Georgia Subclass Members, and RPM's clients are not fully informed as to whether RPM's data security measures have been improved since the Data Breach. By all available measures, RPM's data systems have not been adequately improved, and Plaintiffs and Georgia Subclass Members remain at an unreasonable risk from future cyberattacks.

245. Plaintiffs and the Georgia Subclass, therefore, are entitled to the injunctive relief sought herein because, among other things, RPM continues to retain their PII, future cyber-attacks targeting the same data are foreseeable, and Defendants have not provided sufficient notice identifying any remedial measures that will protect the data from future attack. Moreover, absent injunctive relief, Defendant will continue to misrepresent and imply that its data systems are adequate to protect the PII of Plaintiffs and the Georgia Subclass from future cyberattacks without providing any firm details or basis to support these representations.

246. The Georgia DTPA states that the "court, in its discretion, may award attorney's fees to the prevailing party if . . . [t]he party charged with a deceptive trade practice has willfully engaged in the trade practice knowing it to be deceptive." Ga. Code Ann. § 10-1-373(b)(2). RPM willfully engaged in deceptive trade practices knowing them to be deceptive. RPM knew or should have known that its data security practices were deficient. This is true because, among other things, RPM was aware that entities responsible for collecting and maintaining large amounts of PII, including Social Security numbers and financial information, are frequent targets of sophisticated cyberattacks. RPM knew or should have known that its data security practices were insufficient to guard against those attacks.

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

247. The Georgia DTPA states that "[c]osts shall be allowed to the prevailing party unless the court otherwise directs." Ga. Code Ann. § 10-1-373(b). Plaintiff and the Georgia Subclass are entitled to recover their costs of pursuing this litigation.

248. As a result of RPM's deceptive acts and practices, Plaintiff and the Georgia Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and non-monetary damages, as alleged herein.

249. As a further result of RPM's deceptive acts and practices, Plaintiff and the Georgia Subclass are at future risk of injury as a result of RPM's misrepresentations as to its data security practices and the lack of information RPM has provided regarding any enhancements to its data security.

250. Plaintiff and the Georgia Subclass seek all monetary and non-monetary relief allowed by the Georgia DTPA, including injunctive relief and attorneys' fees.

SIXTH CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT
CAL. CIV. CODE §§ 1798.100, *ET SEQ.* ("CCPA")
(On behalf of Plaintiff Woodruff and the California Subclass)

251. Plaintiff Woodruff incorporates by reference the foregoing paragraphs as if fully set forth herein.

252. Plaintiff Woodruff and members of the California Subclass are consumers as that term is defined in Cal. Civ. Code § 1798.140(g).

253. Defendant is a business as that term is defined in Cal. Civ. Code § 1798.140(c). Defendant is organized or operated for profit or financial benefit of its owner. Defendant collects consumers' personal information (including that of CCPA Plaintiffs and the California Subclass) or such information is collected on Defendant's behalf, and Defendant determines the purposes and means of the processing of consumers' personal information.

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

254. The information accessed during the Data Breach constitutes "personal information" as that term is defined in Cal. Civ. Code § 1798.140(o)(1). At a minimum, that information included names and Social Security numbers.

255. Under the CCPA, Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information that they stored. Cal. Civ. Code § 1798.150(a)(1).

256. Defendant's failure to prevent the Data Breach by implementing and maintaining reasonable security procedures and practices constitutes a breach of their duty under the CCPA.

257. As a result of the Data Breach, the nonencrypted and nonredacted personal information of CCPA Plaintiff and the California Subclass was subject to unauthorized access and exfiltration, theft, or disclosures. The personal information accessed in the Data Breach was nonencrypted and nonredacted as evidenced by the fact that Defendant was required to provide notification letters under the laws of several states that require notification of unauthorized access to nonencrypted and nonredacted information.

258. In accordance with Cal. Civ. Code § 1798.150(b), CCPA Plaintiff provided Defendant with written notice of their alleged violation of Cal. Civ. Code § 1798.150(a). Plaintiff Woodruff mailed notice by certified mail, return receipt requested, on February 24, 2023. *See* Exhibit A. Defendant responded to Plaintiff Woodruff's notice on March 24, 2023. *See* Exhibit B.

259. Defendant did not actually cure the noticed violations. Rather, Defendant's response claims, "any alleged violation of the CCPA against RPM is patently devoid of merit." *See* Exhibit B at p. 1. Outside of remedial security measures, Defendant has not taken any steps to retrieve the information and the response does not provide any assurance that Plaintiff's and California Subclass' Private Information was not viewed by—and/or is still not in the hands of—unauthorized parties.

260. Furthermore, none of the steps Defendant asserts in its response demonstrates an actual cure of its failure to implement reasonable security measures to protect Plaintiff's and

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

California Subclass members' PII, as the vague steps it asserts it has taken are not sufficient to protect Plaintiff's and California Subclass members' PII into the future.

261. Defendant's response is wholly insufficient to demonstrate any "actual cure" of its failure to implement reasonable security to protect Plaintiff's and California Subclass members' information.

262. As Defendant has not "actually cured" the violation, Plaintiff and the California Subclass seek statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

SEVENTH CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW ("UCL")
Cal. Bus. & Prof. Code §§ 17200, *et seq*.
(On behalf of Plaintiff Woodruff and the California Subclass)

263. Plaintiff Woodruff incorporates by reference the foregoing paragraphs as if fully set forth herein.

264. Plaintiff Woodruff and Defendant are "persons" as defined by Cal. Bus. & Prof. Code § 17201.

265. The UCL prohibits "unlawful, unfair, or fraudulent business acts or practices."

266. By failing to take reasonable precautions to protect the PII of Plaintiff and the California Subclass, Defendant has engaged in "unlawful," "unfair," and "fraudulent" business practices in violation of the UCL.

267. First, Defendant engaged in "unlawful" acts or practices because it violated multiple laws, including the California Consumer Records Act, Cal. Civ. Code § 1798.81.5; the FTC Act; and the common law, all as alleged herein.

268. Second, Defendant engaged in "unfair" acts or practices, including the following:

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

a. Defendant failed to implement and maintain reasonable data security measures to protect the California Subclass Members' PII. Defendant failed to identify foreseeable security risks and adequately maintain their data security in light of the known risk of cyber intrusions, especially in light of the highly sensitive nature of the information which Defendant stored. Defendant's conduct, with little if any social utility, is unfair when weighed against the harm to the California Subclass Members whose PII has been compromised.

b. Defendant's failure to implement and maintain reasonable data security measures was contrary to legislatively-declared public policy that seeks to protect consumers' personal information and ensures that entities entrusted with PII adopt appropriate security measures. These policies are reflected in various laws, including the CCPA (Cal. Civ. Code §§ 1798.100 *et seq.*); the FTC Act (15 U.S.C. § 45); and the California Consumer Records Act (Cal. Civ. Code § 1798.81.5).

c. Defendant's failure to implement and maintain reasonable data security measures led to the substantial consumer injuries described herein. These injuries are not outweighed by countervailing benefits to consumers or competition. Moreover, because consumers could not have reasonably known of Defendant's inadequate data security, consumers could not have reasonably avoided the harms that Defendant's conduct caused.

269. *Third*, Defendant engaged in "fraudulent" acts or practices, including, but not limited to, the following:

a. Defendant omitted and concealed the fact that it did not employ reasonable safeguards to protect the PII of Plaintiff and the California Subclass. Defendant could and should have made a proper disclosure of its failure to employ reasonable safeguards prior to contracting to provide services to the companies

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

with whom Plaintiff and the California Subclass Members did business. Defendant also could and should have made a proper disclosure of its failure to employ reasonable safeguards directly to Plaintiff and the California Subclass at the time that it requested or received their PII, or by any other means reasonably calculated to inform the California Subclass of the inadequate data security.

b. Defendant required consumers to provide their PII, either directly or through companies with whom they did business, in order to administer their benefits and payroll. In doing so, Defendant made implied or implicit representations that its data security practices were sufficient to protect consumers' PII. By virtue of accepting consumers' PII, Defendant implicitly represented that its data security procedures were sufficient to safeguard the PII. Those representations were false and misleading.

270. As a direct and proximate result of Defendant's acts of unlawful, unfair, and fraudulent practices and acts, Plaintiff and the California Subclass were injured and lost money or property, and suffered the various types of damages alleged herein.

271. The UCL states that an action may be brought by any person who has "suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Plaintiff and the California Subclass Members suffered injury in fact and lost money or property, including in the form of the loss of value of their breached PII, as a result of Defendant's unfair competition as set forth herein. PII is valuable which is demonstrated by the fact that Defendant's business is built in part by managing the PII of the Class.

272. Plaintiff and the California Subclass are entitled to injunctive relief to address Defendant's past and future acts of unfair competition.

273. Plaintiff and the California Subclass are entitled to restitution of money and property that Defendant obtained by means of unlawful, unfair, or fraudulent practices, and

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

restitutionary disgorgement of all profits accruing to Defendant as a result of its unlawful and unfair business practices.

274. Plaintiff lacks an adequate remedy at law because the injuries here include acurrent and continuing risk of identity theft and fraud that can never be fully remedied through damages.

275. Further, if an injunction is not issued, Plaintiff and California Subclass Members will suffer irreparable injury. The risk of another such breach is real, immediate, and substantial. Plaintiff lacks an adequate remedy at law that will reasonably protect them against the risk of such further breach.

276. Plaintiff and the California Subclass seek all monetary and non-monetary relief available to them under the UCL, including reasonable attorney's fees as allowed under Cal. Code Civ. Proc. §1021.5.

EIGHTH CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT ("CCRA")
CAL. BUS. & PROF. CODE §§ 17200, *ET SEQ.*
(On behalf of Plaintiff Woodruff and the California Subclass)

277. Plaintiff Woodruff incorporates by reference the foregoing paragraphs as if fully set forth herein.

278. The California legislature enacted the California Customer Records Act ("CCRA") to "ensure that personal information about California residents is protected." Cal. Civ. Code § 1798.81.5.

279. The CCRA states that any business which "owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(b) (emphasis added).

280. Under the CCRA, personal information includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following

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

data elements, when either the name or the data elements are not encrypted or redacted: Social Security number, Driver's license number . . . [or] medical information."

281. The personal information compromised in the Data Breach includes information that meets this definition. The information was unencrypted and unredacted as evidenced by the fact that Defendant was required to provide notification letters under the laws of several states that require notification of unauthorized access to unencrypted and unredacted information.

282. Defendant failed to maintain reasonable data security procedures appropriate to the nature of the personal information. Accordingly, Defendant violated Cal. Civ. Code § 1798.81.5(b).

283. Plaintiff Woodruff and the California Subclass were injured by Defendant's violation of Cal. Civ. Code § 1798.81.5(b) and seek damages pursuant to Cal. Civ. Code § 1798.84(b). Plaintiff Woodruff and the California Subclass were injured in the various ways alleged herein. They seek all monetary and non-monetary relief allowed by the CCRA to compensate for their various types of damages alleged herein.

284. Plaintiff Woodruff and the California Subclass are also entitled to injunctive relief pursuant to Cal. Civ. Code § 1798.84(e), including substantial improvements to Defendant's data security systems.

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

285. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

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

287. Defendant owed and owes a duty of care to Plaintiffs and Class Members that require it to adequately secure Plaintiffs' and Class Members' PII.

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

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

289. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members.

290. As such, an actual dispute exists between the rights of Plaintiffs and Class Members on one hand, and the ongoing and future obligations owed by Defendant to Plaintiffs and Class Members, on the other hand, with respect to the security of Plaintiffs' and Class Members' PII in Defendant's possession.

291. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and the members of the Class. Further, Plaintiffs and the members of the Class are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

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

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

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

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

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

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

d. Ordering that Defendant provide employee training regarding the dangers and risks inherent in using file-sharing websites;

e. Ordering that Defendant cease transmitting PII via file-sharing websites;

f. Ordering that Defendant cease storing PII on file-sharing websites;

g. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any PII not necessary for its provision of services;

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

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, personally identifiable information.

PRAYER FOR RELIEF

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

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

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

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

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

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

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

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Class Action Complaint.

Dated: May 4, 2023

TOUSLEY BRAIN STEPHENS PLLC

By: *s/Kaleigh N. Boyd*
Kaleigh N. Boyd, WSBA #52684
Jason T. Dennett, WSBA #30686
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101-3147
Tel: (206) 682-5600
Fax: (206) 682-2992
kboyd@tousley.com
jdennett@tousley.com

Interim Liaison Counsel

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

John A. Yanchunis*
Ryan D. Maxey*
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602

Tel: (813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

Interim Co-Lead Counsel

Nathan D. Prosser*
HELLMUTH & JOHNSON PLLC
8050 West 78th Street
Edina, MN 55439
Tel: (952) 522-4291
nprosser@hjlawfirm.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Tel: (513) 651-3700
tcoates@msdlegal.com
dgould@msdlegal.com

Joseph M. Lyon*
THE LYON FIRM
2754 Erie Ave.
Cincinnati, OH 45208
Tel: (513) 381-2333
jlyon@thelyonfirm.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
221 West Monroe St., Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878
gklinger@milberg.com

William B. Federman*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Tele: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com

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

Samuel J. Strauss, WSBA #46971
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, WI 53703
Tel: (608) 237-1775
Fax: (608) 509-4423
sam@turkestraus.com

Carl v. Malmstrom*
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
11 W. Jackson Street, Suite 1700
Chicago, IL 60604
Tel: (312) 984-0000
malmstrom@whafh.com

Laura Van Note, Esq.*
Cody Alexander Bolce, Esq.*
COLE & VAN NOTE
555 12th St., Ste. 1725
Oakland, CA 94607
Tel: (510) 891-9800
Fax: (510) 891-7030
lvn@colevannote.com
cab@colevannote.com

Mark J. Hilliard, Esq.*
BROTHERS SMITH LLP
2033 N. Main St., Ste. 720
Walnut Creek, CA 94596
Tele: (925) 944-9700
Fax: (925) 944-9701
mhilliard@brotherssmithlaw.com

Bryan Paul Thompson *
CHICAGO CONSUMER LAW CENTER, P.C.
Cook County Firm No. 62709
33 N. Dearborn St., Ste. 400

Chicago, Illinois 60602
Tel: (312) 858-3239
Fax: (312) 610-5646
Bryan.thompson@cclc-law.com

Michael Kind, Esq. (Pro Hac Vice Forthcoming)
Nevada Bar No. 13903
KIND LAW
8860 South Maryland Parkway, Ste. 106
Las Vegas, NV 89123
Tel: (702) 337-2322
Fax: (702) 329-5881
Email: mk@kindlaw.com

Gary E Mason*
Danielle L. Perry*
MASON LLP
5101 Wisconsin Ave., NW, Ste. 305
Washington, D.C. 20016
Tel: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com

Michael C. Submit
FRANK FREED SUBIT & THOMAS LLP
705 Second Ave., Ste. 1200
Seattle, WA 98104
Tel: (206)624-6711
msubit@frankfreed.com
*admitted *pro hac vice*

Additional Counsel for Plaintiffs