Exhibit A1

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

In re TRC Staffing Services, Inc. Data Breach Litigation	Case No. 1:24-cv-02398-VMC

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Nykeema Burke, Jacob Blosser, Tiffany R. Peintner, Ronkavis Young, Latoya Davis, Eli Hargett, Jeanine Keeys, and Adham Elebyany, (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, bring this Class Action Complaint against TRC Staffing Services, Inc. d/b/a TRC Talent Solutions ("Defendant" or "TRC"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII" or "Private Information"), which includes, but is not limited to, the full names and Social Security numbers of approximately 158,593 current and former customers and employees.

2. Defendant is a staffing and personnel solutions company located in Atlanta, Georgia with locations in Florida, Georgia, Missouri, North Carolina, Ohio, and Pennsylvania.

3. In the ordinary course of Defendant's business, Defendant acquires, possesses, analyzes, and otherwise utilizes Plaintiffs' and putative Class Members' PII.

4. By bringing this action, Plaintiffs seek to hold Defendant culpable for the injuries it has caused and will continue to cause Plaintiffs and at least 158,593 other similarly situated persons[1] in the massive and preventable cyberattack purportedly discovered by Defendant on or around May 24, 2024, in which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed and exfiltrated highly sensitive PII belonging to Plaintiffs and Class Members (the "Data Breach").

5. Plaintiffs further seek to hold Defendant responsible for failing to maintain the PII in a manner consistent with industry standards.

6. On or about May 24, 2024, Defendant notified state Attorneys General and many Class Members about the widespread Data Breach (the "Notice Letter").[2]

---

[1] Data Breach Notifications, Office of the Maine Attorney General, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/1adfdecc-df2a-47a6-93bc-ef5a7ad1ac7a.shtml (last accessed October 23, 2024).

[2] Sample Notice Letter available at the Office of the Maine Attorney General, https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/1adfdecc-df2a-47a6-93bc-ef5a7ad1ac7a/b410041f-5e9a-4ff8-9b11-0cd9f6e446c7/TRC%20Staffing%20Services,%20Inc.%20-%20Notice%20of%20Data%20Event%20-%20ME.pdf (last accessed October 23, 2024).

7. The Notice Letter does not explain how the Data Breach occurred, what steps Defendant took following the Data Breach, what changes Defendant has made to its data security, or most importantly, whether Plaintiffs' and Class Members' PII remains in the possession of criminals. The Notice Letter claims TRC is helping victims protect themselves by providing information about how to place a fraud alert or credit freeze on their account and how to sign up for the limited identity monitoring services Defendant offered in response to the Data Breach.

8. By acquiring, utilizing, and benefiting from Plaintiffs' and Class Members' PII for its business and employment purposes, Defendant owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiffs and Class Members to maintain adequate data security measures. These duties required Defendant to design and implement adequate data security systems to protect Plaintiffs' and Class Members' PII in its possession and to keep Plaintiffs' and Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

9. Defendant breached these duties by failing to implement adequate data security measures and protocols to properly safeguard and protect Plaintiffs' and Class Members' PII from a foreseeable cyberattack on its systems that resulted in the unauthorized access and theft of Plaintiffs' and Class Members' PII.

10. Currently, the full extent of the types of PII, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant, its agents, counsel, and forensic security vendors at this phase of the litigation.

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

12. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiffs and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been

compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack; and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

13. Based on the type of targeted criminal activity, the type of PII involved, Defendant's admission that the PII was accessed and stolen, and the claims by a criminal ransomware group that it was responsible for the Data Breach,[3] it can be concluded that the unauthorized criminal third party was able to successfully target Plaintiffs' and Class Members' PII, infiltrate and gain access to Defendant's network, and exfiltrate Plaintiffs' and Class Members' PII, including, at least, full names and Social Security numbers for the purposes of utilizing or selling the PII for use in future fraud and identity theft related cases.

14. The notorious ransomware group, BlackSuit, has claimed responsibility for the Data Breach. "The attack was announced on the [BlackSuit] group's dark web leak site, where they typically post proof of their breaches and ransom demands."[4] As recently reported, "BlackSuit's targeting pattern 'strongly suggests a

[3] *See* https://news.outsourceaccelerator.com/trc-staffing-services-data-breach/ ("The ransomware group BlackSuit has claimed responsibility for the attack.") (last accessed October 23, 2024).

[4] *See* https://ransomwareattacks.halcyon.ai/attacks/the-vulnerabilities-and-tactics-behind-the-ransomware-attack-on-trc-talent-solutions (last accessed November 1, 2024).

financial motivation with a focus on critical sectors that either have smaller cybersecurity budgets or a low tolerance for downtime, thereby increasing the likelihood of a successful attack or a speedy ransom payment.'"[5] according to ReliaQuest.

15. Based on BlackSuit's history of targeting PII and posting on the group's dark web leak site, it is near certain that Plaintiffs' and the Class's PII has been released on the dark web or will be released on the dark web soon.

16. As a result of Defendant's failures and the Data Breach, Plaintiffs' and Class Members' identities are now at a current and substantial imminent and ongoing risk of identity theft and shall remain at risk for the rest of their lives.

17. As Defendant instructed, advised, and warned in its Notice Letter discussed below, Plaintiffs and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time

[5] *See* https://www.extrahop.com/blog/how-revealx-detects-blacksuit-ransomware (quoting ReliaQuest) (last accessed November 1, 2024).

and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

18. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time heeding Defendant's warnings and following its instructions in the Notice Letter; (g) deprivation of value of their PII; (h) invasions of their privacy; and (i) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

19. Plaintiffs bring this action on behalf of all persons whose PII was compromised due to Defendant's failure to adequately protect Plaintiffs' and Class Members' PII. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct and asserts claims on behalf of the Class for Negligence, Negligence per se, Breach of Implied Contract, Unjust Enrichment, Declaratory Judgment, and Violation of O.C.G.A. § 13-6-11.

PARTIES

20. Plaintiff Nykeema Burke is an adult individual and, at all relevant times herein, a resident and citizen of the state of Georgia, residing in Augusta, Georgia, in Richmond County.

21. Plaintiff Jacob Blosser is an adult individual and, at all relevant times herein, a resident and citizen of the state of Georgia, residing in Jefferson, in Jackson County.

22. Plaintiff Tiffany R. Peintner is an adult individual and, at all relevant times herein, a resident and citizen of the state of Oklahoma, residing in Mustang, in Oklahoma County.

23. Plaintiff Ronkavis Young is an adult individual and, at all relevant times herein, a resident and citizen of the state of South Carolina, residing in Prosperity, in Newberry County.

24. Plaintiff Latoya Davis is an adult individual and, at all relevant times herein, a resident and citizen of the state of Georgia, residing in Augusta, in Richmond County.

25. Plaintiff Eli Hargett is an adult individual and, at all relevant times herein, a resident and citizen of the state of North Carolina, residing in Greensboro, in Guilford County.

26. Plaintiff Jeanine Keeys is an adult individual and, at all relevant times

herein, a resident and citizen of the state of North Carolina, residing in Zebulon, in Wake County.

27. Plaintiff Adham Elebyany is an adult individual and, at all relevant times herein, a resident and citizen of the state of Georgia, residing in Lithonia, in DeKalb County.

28. Defendant TRC Staffing Services, Inc. d/b/a TRC Talent Solutions is a domestic for-profit company organized and existing under the laws of the State of Georgia, with its principal place of business at 5909 Peachtree Dunwoody Road, Suite D-1100, Atlanta, GA 30328. TRC Staffing Services, Inc. d/b/a TRC Talent Solutions may be served by service of process upon its registered agent for same, John Brian Robinson, of the same address.

JURISDICTION AND VENUE

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

30. This Court has general personal jurisdiction over Defendant TRC because Defendant's principal place of business is in this District and the acts and

omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

31. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

Background

32. Defendant TRC boasts more than 40 years in operation and success across more than 15 different industries, including technology, healthcare, business services, manufacturing, and more.[6]

33. To provide its staffing services, and in the ordinary course of Defendant's business, Defendant acquires, possesses, analyzes, and otherwise utilizes Plaintiffs' and putative Class Members' PII.

34. Defendant's Privacy Policy, posted on its website, promises "[w]e maintain robust technological and organizational security measures to safeguard your personal information. These measures are designed to prevent accidental loss, unauthorized access, alteration, destruction, or disclosure of your data. Our policy ensures that only individuals with a legitimate business need have access to your personal information. Those handling your data adhere to TRC's IT Information and

[6] *See About*, https://trctalent.com/about/ (last accessed Nov. 4, 2024).

Security rules, data protection guidelines, and other internal policies."[7]

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members

35. In the ordinary course of its business and for employment purposes, TRC maintains the PII of its customers, current and past employees, consumers, and others, including but not limited to: full names, Social Security numbers, addresses, driver's license numbers, state identification numbers, passport numbers, financial account information, health insurance information, and medical information.

36. Additionally, Defendant may receive PII from other individuals and/or organizations including Plaintiffs' and Class Members' employers, insurance carriers, and in connection with enrollment in employee insurance and retirement benefit plans.

37. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to consumers and employees, Defendant, upon information and belief, promises to, among other things: keep protected health information private; comply with industry standards related to data security and PII; inform consumers of its legal duties and comply with all federal and state laws protecting consumer PII; only use and release PII for reasons that relate to medical care and treatment; and provide adequate notice to individuals if their PII is disclosed

[7] *Privacy Policy*, https://trctalent.com/privacy-policy/ (last accessed October 23, 2024).

without authorization.

38. At every step, Defendant acquires and maintains sensitive PII and has a duty to protect that PII from unauthorized access.

39. 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.

40. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

41. Plaintiffs and Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use their PII solely for proper business services and purposes, and to prevent the unauthorized disclosure of their PII.

The Cyberattack and Data Breach

42. Cybercriminals gained access to Defendant's computer systems on or about March 25, 2024 and then maintained this access, unfettered and undetected, until it was discovered on or about April 12, 2024. During this time, the cybercriminals were able to access and exfiltrate sensitive files containing Plaintiffs' and Class Members' full names and Social Security numbers. Upon information and belief, the files exfiltrated in the Data Breach also included Plaintiffs' and Class

Members' contact information, and such information would typically be included in any documents also containing their names and Social Security numbers.

43. The amount of time this intrusion remained undetected evidences a lack of reasonable security measures designed to detect and limit incidents of this nature.

44. Defendant waited until on or about May 24, 2024 to begin sending notices of the Data Breach to Plaintiffs and Class Members.

45. In total, Defendant identified at least 158,593 individuals believed to be impacted by the Data Breach.

46. The sensitive files exfiltrated in the Data Breach were stored in a way that they were unencrypted and vulnerable to access and exfiltration by unauthorized persons.

47. Information security journalists have commented on TRC's data security failures, stating, in relevant part:

> Given the nature of TRC Talent Solutions' business, which involves significant data handling and processing, the company is inherently at risk of cyber-attacks. The integration of various IT systems for talent management and financial services could provide multiple entry points for cybercriminals. The use of VMware ESXi servers, a known target for BlackSuit, might have been a critical factor in the breach.[8]

[8] *See* https://ransomwareattacks.halcyon.ai/attacks/the-vulnerabilities-and-tactics-behind-the-ransomware-attack-on-trc-talent-solutions (last accessed on Nov. 1, 2024).

48. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations to keep Plaintiffs' and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

49. Plaintiffs and Class Members provided their PII directly, or indirectly, to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

50. Through its Notice Letter, TRC also recognized the actual imminent harm and injury that flowed from the Data Breach, and accordingly encouraged breach victims to take steps to mitigate their risk of identity theft, such as reviewing financial accounts, and reviewing credit reports for possible fraud.

51. TRC advised breach victims to "remain vigilant against incidents of identity theft and fraud by reviewing your account and free credit reports for suspicious activity and to detect errors."[9]

52. TRC has offered abbreviated, non-automatic credit monitoring services to victims thereby identifying the harm posed to Plaintiffs and Class Members as a

[9] Sample Notice Letter available at the Office of the Maine Attorney General, https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/1adfdecc-df2a-47a6-93bc-ef5a7ad1ac7a/b410041f-5e9a-4ff8-9b11-0cd9f6e446c7/TRC%20Staffing%20Services,%20Inc.%20-%20Notice%20of%20Data%20Event%20-%20ME.pdf (last accessed October 23, 2024).

result of the Data Breach, which does not adequately address the lifelong harm that victims face following the Data Breach. Indeed, the Data Breach involves PII that cannot be changed, such as Social Security numbers.

53. The Notice Letters stated PII, including full names and Social Security numbers, were accessed and exfiltrated in the Data Breach.

54. As a result of the Data Breach, Plaintiffs and 158,593 Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

55. Defendant waited over over a month to disclose the Data Brach to Plaintiffs and Class Members. As a result of this delay, Plaintiffs and Class Members had no idea their PII had been stolen in the Data Breach, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

56. Defendant's failure to timely detect and report the Data Breach made its consumers and employees vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

57. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class Members.

58. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect its consumers' or employees' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

59. Plaintiffs and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their PII, which includes information that is static, does not change, and can be used to commit a myriad of financial crimes.

60. Plaintiffs and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use their PII for authorized purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand Defendant safeguard their PII.

61. The unencrypted PII of Plaintiffs and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers, particularly cyber attackers like BlackSuit. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval

of Plaintiffs and Class Members. In turn, unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

62. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII.

The Data Breach Was Foreseeable

63. Defendant should be keenly aware that its computer systems were a target for cyber security attacks as it acknowledged in its Privacy Policy the existence of certain policies and procedures that it has specifically put in place to "address data security incidents" when they occur.[10]

64. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in many industries preceding the date of the breach, especially in the staffing industry where sensitive information is commonly exchanged.

65. Because Defendant had duties to protect Plaintiffs' and Class Members' PII, Defendant should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

66. In the years immediately preceding the Data Breach, Defendant knew

[10] https://trctalent.com/privacy-policy/ (last accessed Nov. 4, 2024).

or should have known that TRC's computer systems and network were a target for cybersecurity attacks, including attacks involving data theft, because warnings were readily available and accessible via the internet. In addition to articles in the public press about the extensive number of data breaches affecting companies throughout all industries, governmental agencies have constantly sent and published notices of the need for companies that maintain sensitive personal information to carefully safeguard the sensitive and valuable information collected from consumers.

67. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[11]

68. Indeed, cyberattacks on large corporations like TRC have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, potential attack.[12]

69. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) unauthorized actors were targeting companies such as TRC, (ii) unauthorized actors were

[11] *See* 2021 Data Breach Annual Report, ITRC 6 (Jan. 2022), available at https://www.idtheftcenter.org/notified (last visited Oct. 24, 2024).

[12] *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Oct. 243, 2024).

aggressive in their pursuit of companies such as TRC, (iii) unauthorized actors were leaking corporate information on dark web portals, and (iv) unauthorized actors' tactics included threatening to release stolen data.

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

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

Defendant Had an Obligation to Protect the PII

72. Defendant's failure to adequately secure Plaintiffs' and Class Members' PII breaches duties it owes Plaintiffs and Class Members under statutory and common law. Moreover, Plaintiffs and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard its data, independent of any statute.

73. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has

concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. S*ee, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

74. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

75. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiffs and Class Members.

76. Defendant owed a duty to Plaintiffs and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PII in its possession was adequately secured and protected.

77. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its

possession, including not sharing information with other entities who maintained substandard data security systems.

78. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

79. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

80. Defendant owed a duty to Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

81. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

82. Defendant owed a duty to Plaintiffs and Class Members to encrypt and/or more reliably encrypt Plaintiffs' and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

83. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be

imposed on Plaintiffs and Class Members as a result of a breach.

84. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to, at least, tens of thousands of individuals' PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

Value of PII

85. The PII of individuals remains of high value to criminals, as evidenced by the prices criminals will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[13] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

---

[13] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 24, 2024).

[14] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 24, 2024).

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 24, 2024).

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

87. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[16]

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

89. The fraudulent activity resulting from the Data Breach may not come to light for years as there may be a time lag between when harm occurs versus when it is discovered, and also between when the PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which

[16] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 24, 2024).

conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has 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.[17]

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

91. Plaintiffs and Class Members now face a lifetime of constant surveillance of their financial and personal records, credit monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

92. Defendant has acknowledged the risk and harm caused to Plaintiffs and Class Members as a result of the Data Breach. Defendant, to date, has offered Plaintiffs and Class Members abbreviated, non-automatic credit monitoring services. The limited credit monitoring is inadequate to protect Plaintiffs and Class

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at*: https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 24, 2024).

Members from the threats they face for years to come, particularly in light of the PII at issue here. Moreover, Defendant put the burden squarely on Plaintiffs and Class Members to enroll in the inadequate monitoring services.

Defendant Failed to Properly Protect Plaintiffs' and Class Members' PII

93. 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.

94. 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.

95. 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 from being compromised.

96. 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."[18]

97. 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 their respective lifetimes.

98. 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.
- 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.

[18] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, FED. TRADE COMM., *available at:* https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last visited Oct. 24, 2024).

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for

different organizational units.[19]

99. 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 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

[19] *Protecting Your Networks from Ransomware*, 3-4, U.S. GOV'T., *available at* https://www.justice.gov/criminal/criminal-ccips/file/872771/dl (last visited Nov. 4, 2024).

possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

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

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[20]

100. 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

[20] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited Oct. 24, 2024).

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection;
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[21]

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

102. The occurrence of the Data Breach indicates that Defendant failed to

[21] *See Human-operated ransomware attacks: A preventable disaster*, Microsoft (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Oct. 24, 2024).

adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the theft of the PII of Plaintiffs and Class Members.

103. As a result of computer systems in need of security upgrades and inadequate procedures for handling email phishing attacks, viruses, malignant computer code, and hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII.

104. 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.

Defendant Failed to Comply with Industry Standards

105. As shown above, experts studying cyber security routinely identify companies in the staffing industry as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

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

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

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

109. The foregoing frameworks exist and applicable industry standards in the logistics industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

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

Defendant's Negligent Acts and Breaches

111. Defendant participated in and controlled the process of gathering the

PII from Plaintiffs and Class Members.

112. Defendant therefore assumed and otherwise owed duties and obligations to Plaintiffs and Class Members to take reasonable measures to protect the information, including the duty of oversight, training, instruction, and testing of the data security policies and network systems. Defendant breached these obligations to Plaintiffs and Class Members and/or was otherwise negligent because it failed to properly implement data security systems and policies that would adequately safeguard Plaintiffs' and Class Members' PII. Upon information and belief, Defendant's unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

a. Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiffs' and Class Members' PII;

b. Failing to properly monitor its data security systems for data security vulnerabilities and risk;

c. Failing to test and assess the adequacy of its data security system;

d. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

e. Failing to develop and put into place uniform procedures and data security protections for its network;

f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g. Failing to ensure or otherwise require that it was compliant with FTC

guidelines for cybersecurity;

h. Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;

i. Failing to implement or update antivirus and malware protection software;

j. Failing to require encryption or adequate encryption on its data systems;

k. Otherwise negligently and unlawfully failing to safeguard Plaintiffs' and Class Members' PII provided to Defendant, which in turn allowed cyberthieves to access its IT systems.

COMMON INJURIES & DAMAGES

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

114. 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 imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) theft of their PII; (b) invasion of privacy; (c) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (d) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (e) "out of pocket" costs incurred due to actual identity theft; (f) loss of time incurred due to actual identity theft; (g) loss of time due to increased spam and targeted

marketing emails; (h) the loss of benefit of the bargain (price premium damages); (i) diminution or loss of value of their PII; and (j) 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.

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

115. 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.

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

117. 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.

118. The Dark Web is an unindexed layer of the internet that requires special software or authentication to access.[22] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, Dark Web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[23] This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

119. 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.[24] The digital character of PII stolen in data

---

[22] Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited Oct. 24, 2024).

[23] *Id.*

[24] *What is the Dark Web?* – Microsoft 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last visited Oct. 24, 2024).

breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[25] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[26]

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

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

[25] *Id.*; *see also* Louis DeNicola, *supra* note 22.

[26] *Id.*

can cause a lot of problems.[27]

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

121. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

122. 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

---

[27] Social Security Administration, *Identity Theft and Your Social Security Number* (2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Dec. 13, 2023).

[28] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Oct. 24, 2024).

being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[29]

123. 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.[30]

124. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[31] Defendant did not rapidly report to Plaintiff and Class Members that their PII had been stolen.

125. 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.

126. 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

[29] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 24, 2024).

[30] *See 2019 Internet Crime Report*, FBI (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited Oct. 24, 2024).

[31] *Id.*

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 monitoring their reports for future inaccuracies, closing existing bank/credit accounts, opening new ones, and disputing charges with creditors.

127. 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 remain vigilant against unauthorized data use for years or even decades to come.

128. The Federal Trade Commission ("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."[32]

129. The FTC has also issued numerous guidelines for businesses that

[32] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), FTC (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited Oct. 24, 2024).

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.[33]

130. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout. The FTC treats 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(a) of the FTC Act.[34]

---

[33] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Dec. 13, 2023).

[34] *See, e.g.*, *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices (last visited Oct. 24, 2024).

131. 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.

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

132. As a result of the recognized risk of identity theft, when a Data Breach occurs, an individual is notified by a company that their PII was compromised, as in this Data Breach. The reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm. This is especially true and necessary where, as here, a ransomware group has claimed responsibility for the Data Breach and likely posted Plaintiffs' and Class Members' PII to the dark web.

133. Thus, due to Defendant's admitted recognition of the actual and imminent risk of identity theft, Defendant offered Plaintiffs and Class Members abbreviated, limited, and non-automatic credit monitoring services.

134. Plaintiffs and Class Members have spent, 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, which may take years to discover and detect.

135. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[35]

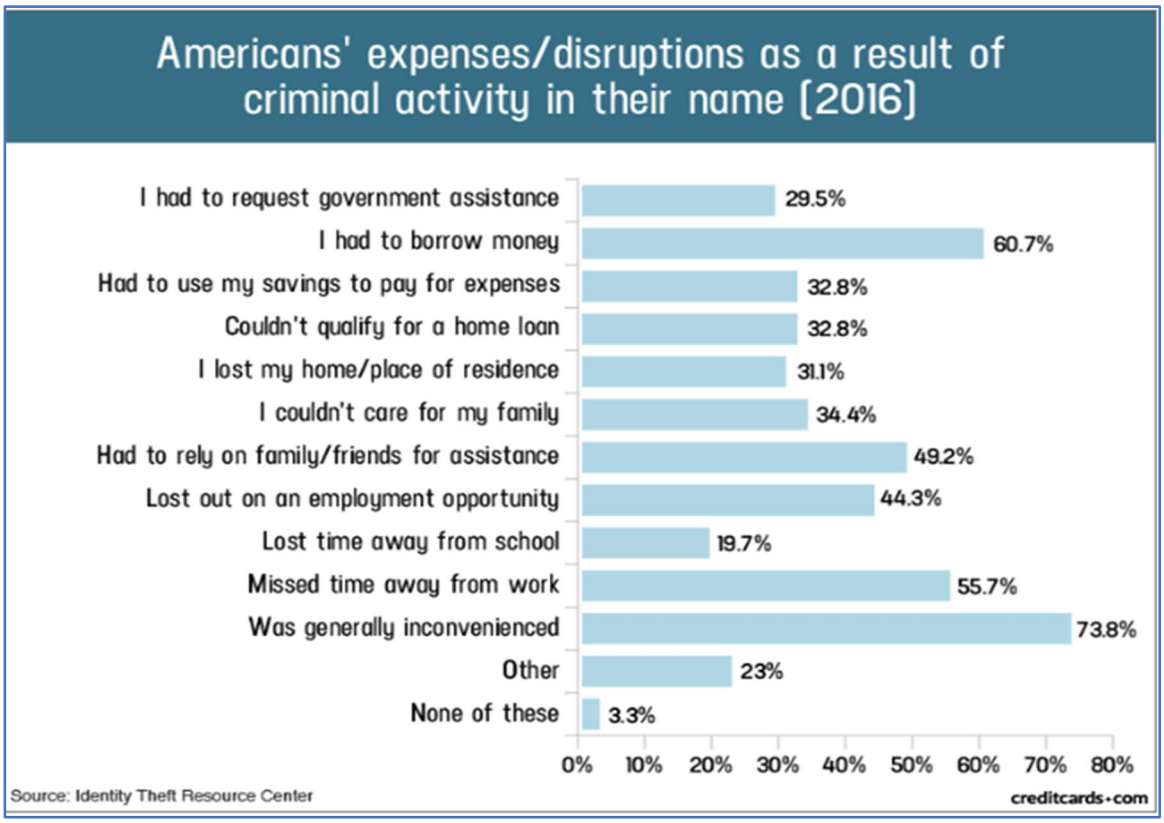
136. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert 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 credit freeze on their credit, and correcting their credit reports.[36]

137. A study by Identity Theft Resource Center shows the multitude of

[35] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007) ("GAO Report"), available at https://www.gao.gov/new.items/d07737.pdf (last visited Oct. 24, 2024).

[36] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Oct. 24, 2024).

harms caused by fraudulent use of personal and financial information:[37]



138. Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit

[37] Jason Steele, *Credit Card and ID Theft Statistics* (Oct. 24, 2017), https://web.archive.org/web/20190304002224/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Oct. 24, 2024).

reports.[38]

Diminution of Value of the PII

139. PII is a valuable property right.[39] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts that include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

140. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII aggregated from the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

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

142. Medical information is especially valuable to identity thieves. Cybersecurity firm Trustwave calculated the black-market value of medical records

---

[38] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Oct. 24, 2024).

[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 Oct. 24, 2024).

at $250 each.[41]

143. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[42] 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.[43, 44] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[45]

144. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

---

[41] Paul Ndrag, *Medical records are the hottest items on the dark web*, Fierce Healthcare (Jan. 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last visited Oct. 24, 2024).

[42] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LA Times (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Oct. 24, 2024).

[43] https://datacoup.com/ (last visited Oct. 24, 2024).

[44] https://digi.me/questions/what-is-a-digi-me-personal-data-vault (last visited Oct. 24, 2024).

[45] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Oct. 24, 2024).

Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

145. 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.

146. The abbreviated, limited, and non-automatic credit monitoring offered to Plaintiffs and Class Members whose PII was stolen is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face ongoing identity theft and financial fraud for the remainder of their lives. Defendant also places the burden squarely on Plaintiffs and Class Members by requiring them to independently sign up for that service, as opposed to automatically enrolling all victims of this Data Breach.

147. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII stolen in the Data Breach, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the PII for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

148. It must be noted there may be a substantial time lag – measured in years

– between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

149. 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.

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

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

152. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year, or more, per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose

[46] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited Oct. 24, 2024).

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.

Injunctive Relief Is Necessary to Protect Against Future Data Breaches

153. 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.

Plaintiffs' Individual Experience

Plaintiff Nykeema A. Burke's Experience

154. Plaintiff Burke entrusted her Private Information to TRC in exchange for staffing services and employment opportunities.

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

156. Plaintiff Burke received a notice letter from Defendant dated May 24, 2024, informing her that her Private Information—including her Social Security number—was specifically identified as having been exposed to cybercriminals in

the Data Breach.

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

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

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

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

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

162. Since the Data Breach, Plaintiff Burke has experienced actual misuse of her Private Information. Specifically, after the Data Breach, Plaintiff Burke received a notification that her Private Information, including her email address, was found on the dark web. Plaintiff Burke attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, and the fact that

she has never experienced anything like this prior to now.

163. As a result of the Data Breach, Plaintiff Burke has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Burke has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing her account statements and other information, reviewing her credit report, and taking other protective and ameliorative steps in response to the Data Breach. Plaintiff Burke has spent approximately 10-20 minutes per day addressing the consequences of the Data Breach since she received her notice letter on May 24, 2024.

164. The letter Plaintiff Burke received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised: "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and free credit reports for suspicious activity and to detect errors."[47] In addition, the

[47] *See* Sample Notice Letter available at the Office of the Maine Attorney General, https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/1adfdecc-df2a-47a6-93bc-ef5a7ad1ac7a/b410041f-5e9a-4ff8-9b11-0cd9f6e446c7/TRC%20Staffing%20Services,%20Inc.%20-

breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[48]

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

166. Plaintiff Burke anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

167. Plaintiff Burke has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Burke's Private Information being placed on the dark web and in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Burke's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in

%20Notice%20of%20Data%20Event%20-%20ME.pdf (last accessed October 23, 2024).

[48] *Id.*

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

Plaintiff Jacob Blosser's Experience

168. Plaintiff Blosser entrusted his Private Information to TRC in order to receive employment services.

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

170. Plaintiff Blosser received a notice letter from Defendant dated May 24, 2024, informing him that his Private Information—including his Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

171. Plaintiff Blosser is very careful about sharing his sensitive information.

172. Plaintiff Blosser stores any documents containing his Private Information in a safe and secure location. Plaintiff Blosser has never knowingly

transmitted unencrypted sensitive PII over the internet or any other unsecured source.

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

174. Plaintiff Blosser has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

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

176. Since the Data Breach, Plaintiff Blosser has experienced data misuse. Indeed, in April, May, and June, Plaintiff Blosser received notifications that his PII had been located on the dark web. Plaintiff Blosser has also noticed an uptick in spam calls and texts. Plaintiff Blosser attributes the foregoing suspicious activity to the Data Breach given these occurrences are unusual and occurred shortly after the Data Breach.

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

of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing his account statements and other information, freezing his credit reports, placing credit alerts with each bureau, changing his passwords, vigilantly checking suspicious calls and texts, and taking other protective and ameliorative steps in response to the Data Breach. Plaintiff Blosser has already spent several hours responding to the Data Breach.

178. The letter Plaintiff Blosser received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised: "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and free credit reports for suspicious activity and to detect errors."[49] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[50]

179. As a result of the Data Breach, Plaintiff Blosser has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of

[49] *Id.*

[50] *Id.*

cybercriminals accessing and misusing his Private Information. Plaintiff Blosser fears that criminals will use his information to commit identity theft.

180. Plaintiff Blosser anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

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

Plaintiff Tiffany R. Peintner's Experience

182. Plaintiff Peintner entrusted her Private Information to TRC in exchange

for staffing services and employment opportunities.

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

184. Plaintiff Peintner received a notice letter from Defendant dated May 24, 2024, informing her that her Private Information—including her Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

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

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

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

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

189. As a result of the Data Breach, which exposed highly valuable

information such as her Social Security number, Plaintiff Peintner is now imminently at risk of crippling future identity theft and fraud.

190. As a result of the Data Breach, Plaintiff Peintner has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Peintner has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing her credit report and other information, responding to and blocking spam phone calls, and taking other protective and ameliorative steps in response to the Data Breach.

191. The letter Plaintiff Peintner received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised: "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and free credit reports for suspicious activity and to detect errors."[51] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with

[51] *Id.*

credit reporting bureaus, and placing security freezes on credit reports.[52]

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

193. Plaintiff Peintner anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

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

[52] *Id.*

undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Ronkavis Young's Experience

195. Plaintiff Young entrusted his Private Information to TRC in exchange for employment.

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

197. Plaintiff Young received a notice letter from Defendant dated May 24, 2024, informing him that his Private Information—including his Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

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

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

200. Because of the Data Breach, Plaintiff Young's Private Information is

now in the hands of cybercriminals.

201. Plaintiff Young has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

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

203. As a result of the Data Breach, Plaintiff Young has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Young has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing his account statements and other information, resecuring his personal computer network, and taking other protective and ameliorative steps in response to the Data Breach.

204. The letter Plaintiff Young received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised: "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your

account and free credit reports for suspicious activity and to detect errors."[53] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[54]

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

206. Plaintiff Young anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

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

[53] *Id.*

[54] *Id.*

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

Plaintiff Latoya R. Davis's Experience

208. Plaintiff Davis entrusted her Private Information to TRC in exchange for employment.

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

210. Plaintiff Davis received a notice letter from Defendant dated May 24, 2024, informing her that her Private Information—including her Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

211. Plaintiff Davis is very careful about sharing her sensitive information. To the best of Plaintiff's knowledge, she has never before had her Private

Information exposed in any other data breach.

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

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

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

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

216. Since the Data Breach, Plaintiff Davis has experienced identity theft in the form of unauthorized charges to her financial accounts. Specifically, Plaintiff has experienced unauthorized charges to her financial accounts for $1,000 and $1,544. Further, since the Data Breach, Plaintiff's credit score has significantly decreased, which has interfered with her ability to purchase a home and make progress towards her financial goals. Plaintiff Davis attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, and the fact that she has never experienced anything like this prior to now.

217. As a result of the Data Breach, Plaintiff Davis has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Davis has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing her account statements and other information, freezing her credit, enrolling in credit monitoring, reviewing alerts from her CerditKarma account, responding to and blocking spam calls and text messages, and taking other protective and ameliorative steps in response to the Data Breach. Plaintiff Davis has spent approximately ten (10) hours responding to the Data Breach.

218. The letter Plaintiff Davis received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised: "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and free credit reports for suspicious activity and to detect errors."[55] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with

[55] *Id.*

credit reporting bureaus, and placing security freezes on credit reports.[56]

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

220. Plaintiff Davis anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

221. In addition to the multiple instances of identity theft and fraud, Plaintiff Davis has suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Davis's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff D Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Davis's Private Information; and (e) continued risk to Plaintiff Davis's

[56] *Id.*

Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Eli Hargett's Experience

222. Plaintiff Hargett entrusted his Private Information to TRC in order to receive employment.

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

224. Plaintiff Hargett received a notice letter from Defendant dated May 24, 2024, informing him that his Private Information—including his Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

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

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

source.

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

228. Plaintiff Hargett has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

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

230. Since the Data Breach, Plaintiff Hargett has experienced a noticeable increase in spam calls and texts.

231. As a result of the Data Breach, Plaintiff Hargett has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Hargett has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, carefully reviewing his account statements and other information, addressing suspicious calls and texts, and taking other protective and ameliorative steps in response to the Data Breach. Plaintiff Hargett has already had to spend multiple hours responding to the Data Breach.

232. The letter Plaintiff Hargett received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised: "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and free credit reports for suspicious activity and to detect errors."[57] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[58]

233. As a result of the Data Breach, Plaintiff Hargett has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information.

234. Plaintiff Hargett anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

235. Plaintiff Hargett has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud

[57] *Id.*

[58] *Id.*

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

Plaintiff Jeanine Keeys' Experience

236. Plaintiff Keeys entrusted her Private Information to TRC in order to receive employment services.

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

238. Plaintiff Keeys received a notice letter from Defendant dated May 24, 2024, informing her that her Private Information—including her Social Security number—was specifically identified as having been exposed to cybercriminals in

the Data Breach.

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

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

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

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

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

244. Since the Data Breach, Plaintiff Keeys has experienced identity theft in the form of unauthorized charges to her financial accounts. Following the Data Breach, Plaintiff Keeys has also received notice that her Private Information has been located on the dark web. Plaintiff Keeys attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, and the fact that

she has never experienced anything like this prior to now.

245. Plaintiff Keeys has also noticed an increase in spam calls and texts in the months following the Data Breach.

246. As a result of the Data Breach, Plaintiff Keeys has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Keeys has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, constantly monitoring her account statements and other information, freezing her credit, enrolling in credit monitoring, placing fraud alerts, addressing fraudulent transactions, addressing spam calls and text messages, and taking other protective and ameliorative steps in response to the Data Breach. Plaintiff Keeys has spent several hours responding to the Data Breach.

247. The letter Plaintiff Keeys received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised: "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and free credit reports for suspicious activity and to detect errors."[59] In addition, the

[59] *Id.*

breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[60]

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

249. Plaintiff Keeys anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

250. Plaintiff Keeys has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Keeys's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff D Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and

[60] *Id.*

deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Keeys's Private Information; and (e) continued risk to Plaintiff Keeys's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant

Plaintiff Adham Elebyany's Experience

251. Plaintiff Elebyany entrusted his Private Information to TRC in order to receive employment services.

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

253. Plaintiff Elebyany received a notice letter from Defendant dated May 24, 2024, informing him that his Private Information—including his Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

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

255. Plaintiff Elebyany stores any documents containing his Private

Information in a safe and secure location. Plaintiff Elebyany has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

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

257. Plaintiff Elebyany has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

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

259. Since the Data Breach, Plaintiff Elebyany has experienced identity theft in the form of unauthorized financial transactions and his tax return being fraudulently redirected to someone else. Plaintiff Elebyany attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, and the fact that he has never experienced anything like this prior to now.

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

consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing his account statements and other information, reviewing his credit report, addressing suspicious calls and texts, contacting the IRS to address the tax fraud he has experienced, and taking other protective and ameliorative steps in response to the Data Breach.

261. The letter Plaintiff Elebyany received from Defendant specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised: "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and free credit reports for suspicious activity and to detect errors."[61] In addition, the breach notification letter listed several "recommended steps" that victims of the Data Breach should take to help protect themselves including, enrolling in credit monitoring, monitoring accounts, reviewing credit reports, placing fraud alerts with credit reporting bureaus, and placing security freezes on credit reports.[62]

262. As a result of the Data Breach, Plaintiff Elebyany has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff

[61] *Id.*

[62] *Id.*

Elebyany fears that criminals will use his information to commit identity theft.

263. Plaintiff Elebyany anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

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

CLASS ALLEGATIONS

265. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and

23(c)(4) of the Federal Rules of Civil Procedure.

266. The nationwide Class that Plaintiffs seeks to represent is defined as follows:

> **All United States residents who were sent a Notice Letter by Defendant TRC Staffing Services, Inc. d/b/a TRC Talent Solutions notifying them that their PII was compromised in the Data Breach.**

267. The nationwide Class is referred to herein as the "Class."

268. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

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

270. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are at least multiple thousands of individuals who were notified by Defendant of the Data Breach. According to the report submitted to the Maine Attorney General's

office, 158,593 individuals had their PII compromised in this Data Breach.[63] The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

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

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;

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

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

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

e. When Defendant actually learned of the Data Breach;

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

[63] Data Breach Notifications, Office of the Maine Attorney General, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/1adfdecc-df2a-47a6-93bc-ef5a7ad1ac7a.shtml (last accessed October 23, 2024).

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

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

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

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

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

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

n. Whether Plaintiffs and Class Members are entitled to expenses of litigation and attorney's fees as a result of Defendant's wrongful conduct; and

o. Whether Plaintiffs and Class Members are entitled to injunctive relief to

redress the imminent and currently ongoing harm faced as a result of the Data Breach.

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

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

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

prosecute this action vigorously.

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

276. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be

recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

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

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

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

281. Likewise, particular issues under Rule 23(c)(4) are appropriate for

certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

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

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

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

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

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

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of

the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

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

CAUSES OF ACTION

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

282. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in 1 through 281.

283. Plaintiffs and the Class entrusted Defendant with their PII.

284. Plaintiffs and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

285. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

286. Defendant knew or reasonably should have known that the failure to

exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

287. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiffs and the Class in Defendant's possession was adequately secured and protected.

288. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain.

289. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Class.

290. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant, either directly or indirectly, with their confidential PII, a necessary part of obtaining services from Defendant.

291. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

292. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

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

294. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Class, including basic encryption techniques freely available to Defendant.

295. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

296. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

297. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendant's possession might have been

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

298. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Class.

299. Defendant has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

300. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendant's possession or control.

301. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

302. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Class in the face of increased risk of theft.

303. Defendant, through its actions and/or omissions, unlawfully breached

its duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of PII.

304. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII that it was no longer required to retain pursuant to regulations.

305. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

306. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Class would not have been stolen.

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

308. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the

compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

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

310. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks

of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

311. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

312. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in 1 through 281.

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

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

315. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly

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

316. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect and the harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

317. The PII of Plaintiffs and the Class was stolen as the proximate result of Defendant's failure to exercise reasonable care in accordance with the standards required by the FTC Act.

318. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is

subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

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

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

321. Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

322. Plaintiffs re-allege and incorporate by reference herein all of the

allegations contained in 1 through 281.

323. The PII of Plaintiffs and Class Members, including full names and Social Security numbers, was provided and entrusted to Defendant.

324. Plaintiffs and Class Members provided their PII to Defendant, either directly or indirectly, through Defendant's clients, as part of Defendant's regular business practices and for Defendant to gain profits.

325. Plaintiffs and the Class entrusted their PII to Defendant. In doing so, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen. As a condition of obtaining services and being employed by Defendant or Defendant's clients, Plaintiffs and Class Members provided and entrusted their PII to Defendant. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

326. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PII to Defendant and/or Defendant's clients with

the reasonable understanding that their PII would be adequately protected by any business associates, like Defendant, from foreseeable threats. This inherent understanding exists independent of any other law or contractual obligation any time that highly sensitive PII is exchanged as a condition of receiving services. It is common sense that but for this implicit and/or explicit agreement, Plaintiffs and Class Members would not have provided their PII.

327. Defendant's contractual obligations are evidenced by its public facing privacy policy, which states:

> We maintain robust technological and organizational security measures to safeguard your personal information. These measures are designed to prevent accidental loss, unauthorized access, alteration, destruction, or disclosure of your data. Our policy ensures that only individuals with a legitimate business need have access to your personal information. Those handling your data adhere to TRC's IT Information and Security rules, data protection guidelines, and other internal policies.[64]

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

329. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that PII was compromised as a result of the Data Breach.

330. As a direct and proximate result of Defendant's above-described breach

[64] *Privacy Policy*, https://trctalent.com/privacy-policy/ (last accessed October 23, 2024).

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

331. As a result of Defendant's breach of implied contract, Plaintiffs and Class Members are entitled to and demand actual, consequential, and nominal damages.

COUNT IV
Unjust Enrichment
(On behalf of Plaintiffs and the Class)

332. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in 1 through 281. Notwithstanding, Plaintiffs bring this claim in the alternative to any claim for breach of contractual obligations.

333. Defendant benefited from receiving Plaintiffs' and Class Members' PII by its ability to retain and use that information for its own benefit, as part of Defendant's business and to gain profits. Defendant understood this benefit.

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

335. Defendant was also enriched from the value of Plaintiffs' and Class Members' PII. PII has independent value as a form of intangible property. Defendant also derives value from this information because it allows Defendant to operate its business and generate revenue.

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

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

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

339. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

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

341. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

342. As a direct and proximate result of Defendant's conduct, Plaintiffs and

Class Members have suffered and will continue to suffer other forms of injury and/or harm.

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

COUNT V
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Class)

344. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in 1 through 281.

345. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and common law described in this Complaint.

346. Defendant owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

347. Defendant still possesses Plaintiffs' and Class Members' PII.

348. Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their

Private Information will occur in the future.

349. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure its current and former employees' Private Information from unauthorized disclosure and theft;

b. Defendant's existing security measures do not comply with its implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect current and former employees' Private Information; and,

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure current and former employees' Private Information.

350. This Court should also issue corresponding prospective injunctive relief Requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect Plaintiffs and Class Members' PII, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members; and,

b. Order that, to comply with Defendant's explicit or implicit contractual

obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response

to a breach;

vii. routinely and continually purging all former employee data that is no longer necessary in order to adequately conduct its business operations; and

viii. meaningfully educating its current and former employees about the threats they face with regard to the security of their Private Information, as well as the steps Defendant's current and former employees should take to protect themselves.

351. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

352. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

353. Issuance of the requested injunction will not disserve the public interest.

To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendant, thus preventing future injury to Plaintiffs and other current and former employees whose Private Information would be further compromised.

COUNT VI
Violation of O.C.G.A. § 13-6-11
(On Behalf of Plaintiffs and the Class)

354. Plaintiff(s) re-alleges and incorporates by reference herein all of the allegations contained in 1 through 281.

355. Defendant through its actions alleged and described herein acted in bad faith, was stubbornly litigious, or caused Plaintiffs and the Class unnecessary trouble and expense with respect to the events underlying this litigation.

356. Section 5 of the FTC Act prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to implement and use reasonable measures to protect PII.

357. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII that it obtained and stored and the foreseeable consequences of a data breach.

358. Defendant also has a duty under the Georgia Constitution ("the

Constitution") which contains a Right to Privacy Clause, Chapter 1, Article 1, to protect the Private Information of Plaintiffs and the Class. The Georgia Constitution states, "no person shall be deprived of life, liberty, or property except by due process of law." Moreover, Georgia law identifies certain invasions of privacy, including the Public Disclosure of Private Life, which prohibits the public disclosure of private facts.

359. This duty to protect Private Information has been recognized by the Georgia Supreme Court in the Restatement of the Law of Torts (Second) §652A, which specifically recognized four common law invasion of privacy claims in Georgia, which include 1) appropriation of likeness; 2) intrusion on solitude or seclusion; 3) public disclosure of private facts; and 4) false light.

360. Defendant's implementation of inadequate data security measures, its failure to resolve vulnerabilities and deficiencies, and its abdication of its responsibility to reasonably protect data it required Plaintiffs and the Class to provide and store on its own servers violates Georgia law.

361. Defendant knew or should have known that it had a responsibility to protect the PII it required Plaintiffs and the Class to provide and stored, that it was entrusted with this PII, and that it was the only entity capable of adequately protecting the PII.

362. Despite that knowledge, Defendant abdicated its duty to protect the PII

it required Plaintiffs and the Class to provide and that it stored.

363. As a direct and proximate result of Defendant's actions, Plaintiffs' and the Class Members' PII was stolen. As further alleged above, the Data Breach was a direct consequence of Defendant's abrogation of data security responsibility and its decision to employ knowingly deficient data security measures that knowingly left the PII unsecured. Had Defendant adopted reasonable data security measures, it could have prevented the Data Breach.

364. As further described above, Plaintiffs and the Class have been injured and suffered losses directly attributable to the Data Breach.

365. Plaintiffs and the Class therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or

disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

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

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

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

iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the

confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

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

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

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

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

x. requiring Defendant to conduct regular database scanning and

securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and Class Members;

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

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats,

both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

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

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

A jury trial is demanded by Plaintiffs and the putative Class Members as to all issues so triable.

Date: November 11, 2024

Respectfully Submitted,

/s/ Kristen Tullos Oliver
Kristen T. Oliver
GA Bar No. 941093
BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, GA 30060
Phone: (678) 227-6375
Fax: (770) 227-6373
E-Mail: ktullos@barneslawgroup.com
Plaintiffs' Interim Liaison Counsel

Mariya Weekes (pro hac vice)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2nd Floor
Coral Gables, FL 33134
Tel: (786) 879-8200
Fax: (786) 879-7520
E-Mail: mweekes@milberg.com

Terence R. Coates (pro hac vice)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700 Fax:
(513) 665-0219
E-Mail: tcoates@msdlegal.com
Plaintiffs Interim Co-Lead Counsel

CERTIFICATE OF SERVICE AND TYPE SIZE COMPLIANCE

I certify that on this date I electronically filed the foregoing **CONSOLIDATED CLASS ACTION COMPLAINT** with the Clerk of Court using the CM/ECF system which will automatically send email notification to all counsel of record. I further certify that the foregoing was prepared in Times New Roman, 14-point font, in compliance with Local Rule 5.1.

Dated: November 11, 2024.

/s/ Kristen Tullos Oliver
Kristen Tullos Oliver
Georgia Bar No. 941093
BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, GA 30060
Telephone: 770-227-6375
Fax: 770-227-6373
E-Mail: ktullos@barneslawgroup.com

Plaintiffs' Interim Liaison Counsel