UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

In re Stanley Steemer International Data Breach Litigation	Case No.: 2:23-cv-03932 **JURY TRIAL DEMANDED**

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Julia Kaled, Phillip Seabrook, Joey Mejia, and Marc Huber (collectively "Plaintiffs"), on behalf of themselves and all others similarly situated, allege the following against Stanley Steemer International, Inc. ("Stanley Steemer" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents, as to all other matters:

NATURE OF THE ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant is a corporation that sells various types of cleaning services across the nation with "approximately 300 operations in 49 states."[1]

3. As part of its business, Defendant stores a litany of highly sensitive personal information about its current and former customers and employees, including names, Social Security numbers, financial account numbers or Credit/Debit Card Number (in combination with

[1] *See* https://www.stanleysteemer.com/about-us/our-story (last visited November 20, 2023).

security code, access code, password or PIN for the account) ("personal identifying information" or "PII").

4. However, on or about February 10, 2023, Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

5. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to the PII of its current and former customers and employees.

6. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the PII of its current and former customers and employees. In short, Defendant's failures placed the PII of its current and former customers and employees in a vulnerable position—rendering them easy targets for cybercriminals.

7. Plaintiff Julia Kaled ("Plaintiff Kaled" or "Ms. Kaled") is a customer of Stanley Steemer and a victim of the Data Breach. Plaintiff Kaled learned of the breach after Defendant reported the incident to Office of the Maine Attorney General, on or about November 15, 2023.[2]

8. Plaintiff Joey Mejia ("Plaintiff Mejia" or "Mr. Mejia") is a customer of Defendant. Mr. Mejia is a Data Breach victim and learned of the breach after receiving a notice of data breach from Defendant, on or about, November 15, 2023. A copy of the Notice of Data Breach received by Plaintiff Mejia is attached as **Exhibit B** ("Mejia's Notice of Data Breach")

[2] *See Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/4256dc2b-46a9-4de9-ad6e-0d61eb204d7b.shtml (last visited Dec. 14, 2023).

9. Plaintiff Phillip Seabrook ("Plaintiff Seabrook" or "Mr. Seabrook") was an employee of Defendant in or around 1996. Mr. Seabrook is a Data Breach victim and learned of the breach after receiving a letter from Defendant, on or about, November 15, 2023.[3]

10. Plaintiff Marc Huber ("Plaintiff Huber" or "Mr. Huber") is a former employee of Defendant. Mr. Huber is a Data Breach victim and learned of the breach after receiving a notice of data breach from Defendant, on or about, November 15, 2023. A copy of the Notice of Data Breach received by Plaintiff Huber is attached as **Exhibit C** ("Huber's Notice of Data Breach")

11. Plaintiffs Kaled, Mejia, Seabrook and Huber bring this class action against Stanley Steemer for its failure to properly secure and safeguard the PII of its current and former customers and employees.

PARTIES

12. Plaintiff Julia Kaled is, and at all times mentioned herein was, an individual citizen of Florida and a customer of Stanley Steemer.

13. Plaintiff Joey Mejia is and at all times mentioned herein was, an individual citizen of California and a customer of Defendant.

14. Plaintiff Phillip Seabrook is, and at all times mentioned herein was, an individual citizen of Ohio and a former employee of Defendant.

15. Plaintiff Marc Huber is an at all times mentioned herein was, an individual citizen of California and a former employee of the Defendant.

16. Defendant Stanley Steemer International, Inc. is an Ohio corporation with its principal place of business at 5800 Innovation Drive, Dublin, Ohio 43016.

[3] *Id.*

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the state of Ohio and have different citizenship from Stanley Steemer, including Plaintiffs. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

18. This Court has jurisdiction over Stanley Steemer because it is headquartered in Ohio, operates in this District, regularly conducts business in Ohio, and has sufficient minimum contacts in Ohio.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Stanley Steemer has harmed Class Members residing in this District.

FACTUAL ALLEGATIONS

Defendant's Business

20. Defendant is an American cleaning company that provides carpet cleaning, tile and grout cleaning, upholstery cleaning, hardwood floor cleaning, air duct cleaning and more.[4]

21. Defendant collects PII from their customers as part of the provision of its services and from their employees as a condition of employment. This PII includes PII which was compromised in the Data Breach alleged herein.

22. Plaintiffs Kaled and Mejia and Class Members are current and former customers of Defendant.

[4] *See* https://www.stanleysteemer.com/about-us/our-story (last visited November 20, 2023).

23. Plaintiffs Seabrook and Huber and Class Members are current and former employees of Defendant.

24. In the course of their relationship with Stanley Steemer, Plaintiffs and Class Members provided Defendant with at least the following: names, Social Security numbers, names and addresses.

25. The information held by Defendant in its computer systems or those of its vendors at the time of the Data Breach included the unencrypted PII of Plaintiffs and Class Members.

26. Upon information and belief, in the course of collecting PII from Plaintiffs and other customers and employees, Defendant promised to provide confidentiality and adequate security for customer data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

27. Indeed, Defendant's Privacy Policy posted on its website provides that: " . . . we use reasonable efforts to protect your personal information from unauthorized access, use, or disclosure . . ."[5]

28. Plaintiffs and Class Members, relied on these promises and on this sophisticated business entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Customers, in general, demand security to safeguard their PII, especially when their Social Security numbers and other sensitive PII is involved.

29. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for

[5] *See* https://www.stanleysteemer.com/privacy-policy#Use (last visited November 20, 2023).

necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

30. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendant has a legal duty to keep consumer's PII safe and confidential.

31. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

32. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

33. 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 disclosure.

Defendant Collected and Stored the PII of Plaintiffs and the Class

34. Upon information and belief, current and former customers and employees of Defendant are required to entrust Defendant, directly or indirectly, with sensitive, non-public PII, without which Defendant could not perform its regular business activities. Defendant retains this information for years and even after the customer relationship has ended.

35. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard their PII from unauthorized access and intrusion.

36. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed 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 PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party.

37. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

38. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

39. Plaintiffs and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data

was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

40. Plaintiffs seek remedies including, but not limited to, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

41. Plaintiffs also seek injunctive and equitable relief to prevent future injury on behalf of themselves and the putative Class.

Defendant Acquires, Collects, And Stores Customers' PII

42. Defendant acquires, collects, shares, and stores a massive amount of its current and former customers' PII.

43. As a condition of using Stanley Steemer's services, Defendant requires that current and former customers entrust it with highly sensitive personal information.

44. Defendant retains and stores this information and derives a substantial economic benefit from the PII that they collect from its customers. But for the collection of PII, Defendant would be unable to offer services to customers like Plaintiffs Kaled and Mejia and Class Members.

45. By obtaining, collecting, and using customer PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting its customers' PII from disclosure.

46. Defendant's customers, like Plaintiffs Kaled and Mejia and putative Class Members, have taken reasonable steps to maintain the confidentiality of their PII and would not have entrusted it to Defendant absent a promise to safeguard that information.

47. Defendant's customers, like Plaintiffs Kaled and Mejia and putative Class Members, relied on Defendant to keep their PII confidential and securely maintained, to use this

information for business purposes only, and to make only authorized disclosures of this information.

Defendant Acquires, Collects, And Stores PII of Current and Former Employees

48. Defendant acquires, collects, shares, and stores a massive amount of its current and former employees' PII.

49. As a condition of obtaining employment, Defendant requires that prospective employees entrust it with highly sensitive personal information.

50. Defendant retains and stores this information and derives a substantial economic benefit from its employees' PII that they collect. But for the collection of its employees' PII, Defendant would be unable to offer employment to its employees like Plaintiffs Seabrook and Huber and members of the Class.

51. By obtaining, collecting, and using the PII of its employees, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII of its employees like Plaintiffs Seabrook and Huber and members of the Class Members' PII from disclosure.

52. Defendant's employees, like Plaintiffs Seabrook and Huber and members of the putative Class, have taken reasonable steps to maintain the confidentiality of their PII and would not have entrusted it to Defendant absent a promise to safeguard that information.

53. Defendant's employees, like Plaintiffs Seabrook and Huber and members of the putative Class, relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach

54. Defendant has disclosed that between February 10, 2023, and March 6, 2023, Defendant was hacked—i.e., for a full twenty-four (24) days.[6]

55. According to Stanley Steemer's report filed with the Office of the Maine Attorney General, on or about November 15, 2023, the compromised PII of Plaintiffs and Class Members included individuals' name, Social Security number, driver's license number, and financial account information.[7]

56. Worryingly, Defendant has admitted that an "unauthorized actor had the ability to access and acquire certain files while on the network."[8]

57. Defendant failed to adequately protect Plaintiffs' and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect the sensitive data of its customers and employees. Hackers targeted and obtained Plaintiffs' and putative Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

58. In total, Defendant injured at least 66,978 persons—via the exposure of their PII—in the Data Breach.[9] Upon information and belief, these 66,978 persons include its current and former customers, employees, and its employees' dependents.

---

[6] *See* **Exhibit A.**

[7] *Data Breach Notifications*, MAINE ATTY GEN, https://apps.web.maine.gov/online/aeviewer/ME/40/4256dc2b-46a9-4de9-ad6e-0d61eb204d7b.shtml (last visited Dec. 14, 2023).

[8] *Id.*

[9] *Id.*

59. Defendant "became aware" of its Data Breach on March 6, 2023.[10]

60. And yet, Defendant waited until November 15, 2023, before it began notifying the class—an inexplicable 254 days *after* Defendant became aware of the Data Breach.[11]

61. Thus, Defendant kept Plaintiffs and the putative Class in the dark—thereby depriving them the opportunity to try and mitigate their injuries in a timely manner.

62. And when Defendant did notify Plaintiffs and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class:

a. "remain vigilant against incidents of identity theft and fraud;"
b. "review[] your account statements;"
c. "monitor[] your credit reports for any unauthorized or suspicious activity;"
d. "educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General."[12]

63. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread injury and monetary damages.

64. Since the breach, Defendant "took steps to enhance our existing security protocols."[13] These steps are too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

---

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*

65. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

66. Further, the Notice of Data Breach shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when.

67. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiffs and putative Class members for the injuries that Defendant inflicted upon them.

68. Because of Defendant's Data Breach, the sensitive PII of Plaintiffs and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages.

69. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, (2) gained actual access to sensitive data, and (3) successfully obtained "the ability to . . . acquire certain files."[14]

70. Omitted from the Notice of Data Breach were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and putative Class Members, who retain a vested interest in ensuring that their PII remains protected.

71. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with

[14] *Id*.

any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

72. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, Defendant failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive PII.

73. The attacker accessed and acquired files on Defendant's network containing unencrypted PII of Plaintiffs and Class Members, including their Social Security numbers and other sensitive information. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach.

74. Plaintiffs further believe their PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

75. Due to the actual and imminent risk of identity theft as a result of the Data Breach, Plaintiffs and Class Members must, as Defendant's Notice of Data Breach encourages, monitor their financial accounts for many years to mitigate the risk of identity theft.

76. In the Notice of Data Breach, Defendant makes an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face well in excess of two years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure

of Plaintiffs' and Class Members' PII.

77. That Defendant is encouraging its current and former customers and employees to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted individuals' PII was acquired, thereby subjecting Plaintiffs and Class Members to a substantial and imminent threat of fraud and identity theft.

78. Defendant had obligations created by the FTC Act, contract, common law, and industry standards to keep Plaintiffs' and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

79. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[15]

80. Thus, on information and belief, Plaintiffs' and the putative Class's stolen PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiff Julia Kaled's Experience

81. Plaintiff Julia Kaled is a former Stanley Steemer customer who received cleaning services from Stanley Steemer in or about 2019 and 2022.

82. Ms. Kaled provided her PII to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her PII. If Ms. Kaled had known that Defendant would not adequately protect her PII, she would not have entrusted Defendant with her PII or allowed Defendant to maintain or use this sensitive PII.

---

[15] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

83. In order to receive services from Stanley Steemer, Plaintiff Kaled was required to provide her PII to Defendant, including her name, Social Security number and address.

84. At the time of the Data Breach—approximately February 10, 2023, through March 6, 2023—Defendant retained Plaintiff Kaled's PII in its system.

85. Plaintiff Kaled is very careful about sharing her sensitive PII. Plaintiff Kaled stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Kaled would not have entrusted her PII to Defendant had she known of Defendant's lax data security policies.

86. Plaintiff Kaled learned of the breach after Defendant reported the incident to Office of the Maine Attorney General, on or about November 15, 2023.[16]

87. According to the report, Plaintiff Kaled's PII was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number and address.

88. In fact, Plaintiff Kaled, suffered injury from a spike in spam and scam calls and text messages following the Data Breach.

89. As a result of the Data Breach, and at the direction of Defendant's Notice of Data Breach, Plaintiff Kaled made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice of Data Breach. Plaintiff Kaled has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

90. Plaintiff Kaled suffered actual injury from having her PII compromised as a result

[16] *See* **Exhibit A**

of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in 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.

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

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

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

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

Plaintiff Joey Mejia's Experience

95. Plaintiff Joey Mejia is a former Stanley Steemer customer who received cleaning services from Stanley Steemer in or about 2019 and 2022.

96. Mr. Mejia provided his PII to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to

protect his PII. If Mr. Mejia had known that Defendant would not adequately protect his PII, he would not have entrusted Defendant with his PII or allowed Defendant to maintain or use this sensitive PII.

97. In order to receive services from Stanley Steemer, Plaintiff Mejia was required to provide PII to Defendant, including his name, Social Security number and address.

98. At the time of the Data Breach—approximately February 10, 2023, through March 6, 2023—Defendant retained Plaintiff Mejia's PII in its system.

99. Plaintiff Mejia is very careful about sharing his sensitive PII. Plaintiff Mejia stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Mejia would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

100. Plaintiff Mejia learned of the breach after receiving a letter from Defendant, on or about, November 15, 2023, which told him that his PII had been accessed during the Data Breach. The Notice of Data Breach informed him that the PII compromised included his Social Security number, driver's license number, and financial account information.

101. As a result of the Data Breach, and at the direction of Defendant's Notice of Data Breach, Plaintiff Mejia made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice of Data Breach. Plaintiff Mejia has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

102. Plaintiff Mejia suffered actual injury from having his PII compromised as a result

of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

103. Plaintiff Mejia suffered actual injury in the form of identity theft. On or about February 15, 2023, Plaintiff was notified that an unidentified third party received a US Bank loan for $30,000 in his name. Plaintiff Mejia is currently disputing the loan and has suffered unjust consequences as a result, including a decrease in his credit score and having to cancel a planned family vacation. In addition, Mr. Mejia has noticed multiple hard inquiries on his credit report which he did not authorize.

104. The Data Breach has caused Plaintiff Mejia to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

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

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

107. Plaintiff Mejia has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and

safeguarded from future breaches.

Plaintiff Phillip Seabrook's Experience

108. Plaintiff Phillip Seabrook was an employee of Stanley Steemer in 1996.

109. Mr. Seabrook provided his PII to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his PII. If Mr. Seabrook had known that Defendant would not adequately protect his PII, he would not have entrusted Defendant with his PII or allowed Defendant to maintain or use this sensitive PII.

110. In order to become a prospective employee of Stanley Steemer, Plaintiff Seabrook was required to provide his PII to Defendant, including his name, Social Security number, and address.

111. At the time of the Data Breach—approximately February 10, 2023, through March 6, 2023—Defendant retained Plaintiff Seabrook's PII in its system.

112. Plaintiff Seabrook is very careful about sharing his sensitive PII. Plaintiff Seabrook stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Seabrook would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

113. Plaintiff Seabrook learned of the breach after receiving a letter from Defendant, on or about, November 15, 2023, which told him that his PII had been accessed during the Data Breach. The Notice of Data Breach informed him that the PII compromised included his Social Security number, driver's license number, and financial account information.

114. As a result of the Data Breach, and at the direction of Defendant's Notice of Data

Breach, Plaintiff Seabrook made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice of Data Breach. Plaintiff Seabrook has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

115. Plaintiff Seabrook suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

116. The Data Breach has caused Plaintiff Seabrook to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

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

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

119. Plaintiff Seabrook has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and

safeguarded from future breaches.

Plaintiff Marc Huber's Experience

120. Plaintiff Marc Huber was employed by Stanley Steemer approximately 32 years ago.

121. At the time of the Data Breach—approximately February 10, 2023, through March 6, 2023—Defendant retained Plaintiff Huber's PII in its system.

122. Defendant was negligent—and unnecessarily maintained Plaintiff Huber's PII for over *three decades*.

123. As a result, Plaintiff Huber was injured by Defendant's Data Breach.

124. As a condition of his employment with Defendant, Plaintiff Huber was required to provide his PII, including but not limited to his full name Social Security number, and address.

125. Defendant used that PII to facilitate its employment of Plaintiff Huber, including payroll, and required Plaintiff Huber to provide that PII in order to obtain employment and payment for that employment.

126. Plaintiff provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

127. Plaintiff reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII.

128. Defendant deprived Plaintiff of the earliest opportunity to guard his PII against the Data Breach's effects by failing to notify him about it for over eight months.

129. Plaintiff Huber is very careful about sharing his sensitive PII. Plaintiff Huber

stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Huber would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

130. On or about, November 15, 2023 Plaintiff Huber received Defendant's Notice of Data Breach which states that after a "diligent and comprehensive review of the contents of the files" which the cybercriminals were able to "access and acquire," Stanley Steemer "determined that the files contained certain information related to you." The Notice specifically states that, as to Plaintiff Huber, these files included his "date of birth and Social Security number."[17]

131. In fact, due to the Data Breach, Plaintiff has *already* experienced multiple instances of fraud, including the use of his Visa debit card, which was used on or about May 15, 2023 to make a fraudulent purchase at Wal-Mart for $10.31 and again on or about May 17, 2023 for $17.27. These fraudulent transactions indicate that the PII of Plaintiff Huber, which was collected and stored by Defendant, was stolen and is in the hands of cybercriminals.

132. Additionally, Plaintiff Huber suffered injury from a spike in spam and scam calls and text messages following the Data Breach.

133. As a result of the Data Breach, and at the direction of Defendant's Notice of Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice of Data Breach. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

---

[17] *See* **Exhibit C.**

134. Plaintiff Huber has and will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft and financial harm. Plaintiff Huber fears for his personal financial security and uncertainty over what PII exposed in the Data Breach. Plaintiff Huber has and will continue to experience feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience.

135. Plaintiff Huber suffered actual injury from the exposure of his PII—which violates his rights to privacy.

136. Plaintiff Huber has suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

137. Plaintiff Huber has suffered imminent and impending injury arising from the substantially increased risk of physical danger, fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties, including cybercriminals, hostile government actors, and terrorists.

138. The Data Breach has caused Plaintiff Huber to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

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

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

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

Plaintiffs and the Proposed Class Face Substantial Risk of Additional Harm

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

143. The ramifications of Defendant's failure to keep Plaintiffs' and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, date of birth, Social Security number, or driver's license number, without permission, to commit fraud or other crimes.

144. The types of PII compromised and potentially stolen in the Data Breach is highly valuable to identity thieves. The stolen PII can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

145. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

146. Identity thieves can also use the stolen data to harm Plaintiffs and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial

> costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health- related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

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

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

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

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

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

Value Of Personally Identifiable Information

148. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[18] 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."[19]

149. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[20]

150. For example, PII can be sold at a price ranging from $40 to $200.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

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

---

[18] 17 C.F.R. § 248.201 (2013).
[19] *Id.*
[20] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed November 20, 2023).
[21] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed November 20, 2023).
[22] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited November 20, 2023).

152. 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 . . . [is] worth more than 10x on the black market."[23]

153. 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.

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

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[24]

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

---

[23] 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 accessed November 20, 2023).

[24] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed November 20, 2022).

The PII That Was Stolen in This Data Breach is Valuable Intangible Property

157. The PII at issue in this case is valuable intangible property. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained. Other reports show that personal information can be sold at a price ranging from $40 to $200.[25] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[26]

The Data Breach Increases Victims' Risk Of Identity Theft

158. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

159. The unencrypted PII of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. 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. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

160. 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.

161. Because a person's identity is akin to a puzzle with multiple data points, the more

---

[25] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 27, 2021).

[26] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the- dark-web/ (last visited Oct. 27, 2021).

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.

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

163. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[27]

164. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

[27] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last accessed on November 20, 2023).

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

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

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

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

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

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

170. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and putative Class Members must, as Defendant's Notice of Data Breach encourages them, monitor their

financial accounts for many years to mitigate the risk of identity theft.

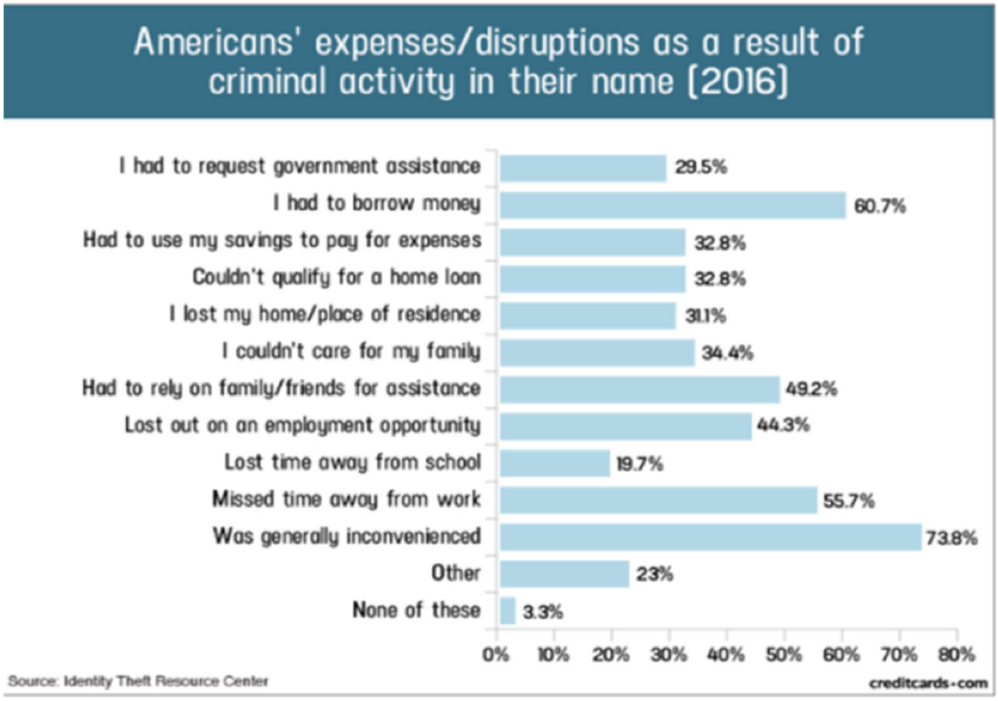
171. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach Notice upon receipt.

172. These 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."[28]

173. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[29]

174. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[30]

[28] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[29] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited November 20, 2023).
[30] Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited November 20, 2023).



175. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[31]

Diminished Value Of PII

176. PII is a valuable property right.[32] Its value is axiomatic, considering the value of "Big Data" in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

[31] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last accessed November 20, 2023) ("GAO Report").
[32] *See, e.g.,* Randall 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).

177. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[33]

178. 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.[34,35]

179. Consumers who agree to provide their web browsing history to Nielsen Corporation can receive up to $50.00 a year.[36]

180. Conversely, sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[37]

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

182. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information

---

[33] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed November 20, 2023).
[34] https://datacoup.com/ (last accessed November 20, 2023).
[35] https://worlddataexchange.com/about (last accessed November 20, 2023).
[36] Nielsen Computer & Mobile Panel, *Frequently Asked Questions, available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed November 20, 2023).
[37] *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 accessed November 20, 2023).

compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

183. 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.

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

185. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, 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.

186. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to over one million individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

187. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

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

188. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity

theft crimes –*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

189. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her 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.

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

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

Data Breaches Are Preventable

192. Defendant could have prevented this Data Breach by, among other things, properly encrypting PII being shared with its vendors or otherwise ensuring that such PII was protected while in transit or accessible.

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

194. The unencrypted PII of putative Class Members will end up for sale to identity

thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

195. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[38]

196. To prevent and detect cyber-attacks and/or ransomware 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, customers and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

[38] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited November 20, 2023).

- 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.[39]

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

Secure internet-facing assets

- Apply 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

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

- 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].[40]

198. Given that Defendant was storing and sharing the PII of its current and former customers and employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

199. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of more than sixty-six thousand current and former customers and employees of Defendant, including that of Plaintiffs and Class Members.

Defendant Knew or Should Have Known of the Risk Because Companies In Possession Of PII Are Particularly Suspectable To Cyber Attacks

200. Defendant's data security obligations were particularly important given the

[40] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited August 9, 2023).

substantial increase in cyber-attacks and/or data breaches targeting companies that collect and store PII, like Defendant, preceding the date of the breach.

201. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

202. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[41]

203. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[42]

204. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[43]

205. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January

[41] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[42] *Id*.
[43] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed November 20, 2023).

2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

206. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

207. 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.

208. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members 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.

209. Additionally, as companies became more dependent on computer systems to run their business,[44] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[45]

210. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially over one million

[44] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last accessed November 20, 2023).
[45] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last accessed November 20, 2023).

individuals' detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

211. In the Notice of Data Breach, Defendant offers to cover credit monitoring services for a period of 24 months. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity and/or credit monitoring services.

212. Defendant's offer of credit and identity monitoring establishes that Plaintiffs' and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

213. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

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

215. As a company in possession of its current and former customers' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by their customers, like Plaintiffs Kaled and Mejia, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on their customers as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent

the Data Breach.

216. As a company in possession of its current and former employees' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff Seabrook and Huber and putative Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff Seabrook and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Stanley Steemer Failed to Comply with FTC Guidelines

217. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, 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 Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

218. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being

transmitted from the system, and have a response plan ready in the event of a breach.

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

220. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

221. These FTC enforcement actions include actions against insurance companies, like Defendant.

222. As evidenced by the Data Breach, Stanley Steemer failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Stanley Steemer's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

223. Stanley Steemer was at all times fully aware of its obligation to protect the PII of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Stanley Steemer Failed to Comply with Industry Standards

224. As noted above, experts studying cybersecurity routinely identify companies like

Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

225. Some industry best practices that should be implemented by companies dealing with sensitive PII, like Stanley Steemer, include but are not limited to: educating all customers, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which customers can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

226. Other best cybersecurity practices that are standard include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

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

228. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Stanley Steemer Breached its Duty to Safeguard Plaintiffs' and Class Members' PII

229. In addition to its obligations under federal and state laws, Stanley Steemer owed

a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Stanley Steemer owed a duty to Plaintiffs and Class Members to provide reasonable security, including compliance with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Class Members

230. Stanley Steemer breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Stanley Steemer's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;
b. Failing to adequately protect current and former customer PII;
c. Failing to adequately protect current and former employee PII;
d. Failing to properly monitor its own data security systems for existing intrusions;
e. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;
f. Failing to sufficiently train its customers and vendors regarding the proper handling of its customers' PII;
g. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;
h. Failing to adhere to the industry standards for cybersecurity as discussed above;

and

i. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' PII.

231. Stanley Steemer negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted PII.

232. Had Stanley Steemer remedied the deficiencies in its information storage and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

CLASS ACTION ALLEGATIONS

233. Plaintiffs bring this action on behalf of themselves and as a class action under Fed. R. Civ. P 23(a) and (b), on behalf of the following proposed Classes:

> **Employee Class:** All former and current employees Defendant has identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").
>
> **Customer Class:** All former and current customers, Defendant has identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").
>
> **California Subclass:** All residents of California, Defendant has identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class")

234. Excluded from the Classes are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

235. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes, as well as add subclasses, before the Court determines whether certification is appropriate.

236. The proposed Classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

237. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time it is likely hundreds, if not thousands of individuals had their PII compromised in this Data Breach, given the Defendant operates widely throughout the United States. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

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

a. Whether Stanley Steemer engaged in the conduct alleged herein;

b. Whether Stanley Steemer's conduct violated the FTCA;

c. When Stanley Steemer learned of the Data Breach;

d. Whether Stanley Steemer's response to the Data Breach was adequate;

e. Whether Stanley Steemer unlawfully lost or disclosed Plaintiffs' and Class Members' PII;

f. Whether Stanley Steemer failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

g. Whether Stanley Steemer's data security systems prior to and during the Data

Breach complied with applicable data security laws and regulations;

h. Whether Stanley Steemer's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Stanley Steemer owed a duty to Class Members to safeguard their PII;

j. Whether Stanley Steemer breached its duty to Class Members to safeguard their PII;

k. Whether hackers obtained Class Members' PII via the Data Breach;

l. Whether Stanley Steemer had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether Stanley Steemer breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

n. Whether Stanley Steemer knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiffs and Class Members suffered as a result of Stanley Steemer's misconduct;

p. Whether Stanley Steemer's conduct was negligent;

q. Whether Stanley Steemer was unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a

constructive trust.

239. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, inter alia, all Class Members were injured through the common misconduct of Stanley Steemer. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to the Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

240. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

241. Predominance. Stanley Steemer has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Stanley Steemer's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

242. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual

Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Stanley Steemer. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

243. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Stanley Steemer has acted and/or refused to act on grounds generally applicable to the Classes such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Classes as a whole.

244. Finally, all members of the proposed Classes are readily ascertainable. Stanley Steemer has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Classes)

245. Plaintiffs hereby repeat and reallege paragraphs 1 through 244 of this Complaint and incorporate them by reference herein.

246. Defendant requires its customers, including Plaintiffs Kaled and Mejia, as well as members of the Customer Class, to submit non-public PII in the ordinary course of providing cleaning services.

247. Defendant requires its employees, including Plaintiffs Seabrook and Huber, as well as members of the Employee Class, to submit non-public PII in the ordinary course of establishing employment.

248. Defendant gathered and stored the PII of its customers as part of its business of soliciting its services to its customers, which solicitations and services affect commerce.

249. Defendant gathered and stored the PII of its current and former employees as part of its practice for offering employment.

250. Plaintiffs and Class Members entrusted Defendant with their PII, directly or indirectly, with the understanding that Defendant would safeguard their information.

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

252. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

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

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

255. Defendant's duty of care to use reasonable security measures arose as a result of the

special relationship that existed between Defendant, Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Classes entrusted Defendant with their confidential PII, a necessary part of being customers or employee of Defendant.

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

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

258. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' and former employees' PII it was no longer required to retain pursuant to regulations.

259. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Classes of the Data Breach.

260. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiffs and the Classes 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 Classes to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

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

a. Failing to adopt, implement, and maintain adequate security measures to safeguard

Class Members' PII;

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

c. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

d. Allowing unauthorized access to Class Members' PII;

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

f. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations;

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

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

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

262. 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 Plaintiffs and the Classes.

263. Plaintiffs and Class Members were within the class of persons the FTC Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm

these statues were intended to guard against.

264. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

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

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

267. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the insurance industry.

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

269. Plaintiffs and the Classes 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 Classes, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

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

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

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

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

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

275. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Classes, the PII of Plaintiffs and the Classes would not have been compromised.

276. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Classes and the harm, or risk of imminent harm, suffered by Plaintiffs and the Classes. The PII of Plaintiffs and the Classes 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.

277. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Classes have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

278. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Classes 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.

279. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Classes 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.

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

281. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

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

COUNT II
Breach of Implied Contract
(On Behalf Of Plaintiffs And the Classes)

283. Plaintiffs hereby repeat and reallege paragraphs 1 through 244 of this Complaint and incorporate them by reference herein.

284. Plaintiffs Kaled and Mejia, as well as the members of the Customer Class were required to provide their PII to Defendant as a condition of being customers of Defendant.

285. Plaintiffs Seabrook and Huber, as well as the members of the Employee Class were required to provide their PII to Defendant as a condition of employment with Defendant.

286. Plaintiffs and the Classes entrusted their PII to Defendant. In so doing, Plaintiffs and the Classes 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 Classes if their data had been breached and compromised or stolen.

287. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

288. At the time Defendant acquired the PII of Plaintiffs and the Classes, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

289. Implicit in the agreements between Plaintiffs and Class Members and Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

290. Plaintiffs and the Classes would not have entrusted their PII to Defendant had they

known that Defendant would make the PII internet-accessible, not encrypt sensitive data elements such as Social Security numbers, and not delete the PII that Defendant no longer had a reasonable need to maintain it.

291. Plaintiffs and the Classes fully performed their obligations under the implied contracts with Defendant.

292. Defendant breached the implied contracts they made with Plaintiffs and the Classes by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Classes once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised because of the Data Breach.

293. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Classes 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.

294. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Classes are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT III
Breach Of Fiduciary Duty
(On Behalf Of Plaintiffs And the Classes)

295. Plaintiffs hereby repeat and reallege paragraphs 1 through 244 of this Complaint and incorporate them by reference herein.

296. In providing their PII, directly or indirectly, to Defendant, Plaintiffs and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiffs and class members to safeguard and keep confidential that PII.

297. Defendant accepted the special confidence Plaintiffs and Class members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiffs' and Class Members' personal information as detailed in its Privacy Policy.

298. In light of the special relationship between Defendant and Plaintiffs and Class members, whereby Defendant became a guardian of Plaintiffs' and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for the benefit of its customers, including Plaintiffs and Class members, for the safeguarding of Plaintiffs' and Class members' PII.

299. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of its relationship with Defendants' customers and employees, in particular, to keep secure the PII of its customers and employees.

300. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to protect the integrity of the systems containing Plaintiffs' and Class members' PII.

301. Defendant breached its fiduciary duties to Plaintiffs and class members by otherwise failing to safeguard Plaintiffs' and Class members' PII.

302. As a direct and proximate result of Defendant's breaches of its fiduciary duties,

Plaintiffs and class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

303. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV
Breach Of Confidence
(On Behalf Of Plaintiffs And the Classes)

304. Plaintiffs hereby repeat and reallege paragraphs 1 through 244 of this Complaint and incorporate them by reference herein.

305. At all times during Plaintiffs' and Class members' interactions with Defendant, Defendant was fully aware of the confidential, novel, and sensitive nature of Plaintiffs' and the Class members' PII that Plaintiffs and Class members provided to Defendant.

306. As alleged herein and above, Defendant's relationship with Plaintiffs and Class members was governed by expectations that Plaintiffs' and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

307. Plaintiffs and Class members provided their respective PII to Defendant, directly or indirectly, with the explicit and implicit understandings that Defendant would protect and not

permit the PII to be disseminated to any unauthorized parties.

308. Plaintiffs and Class members also provided their respective PII to Defendant with the explicit understanding that Defendant would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of information security practices.

309. Defendant voluntarily received in confidence Plaintiffs' and Class members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

310. Due to Defendant's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiffs' and Class members' PII, Plaintiffs' and Class members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class members' confidence, and without their express permission.

311. But for Defendant's disclosure of Plaintiffs' and Class members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' PII, as well as the resulting damages.

312. The injury and harm Plaintiffs and Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class members' PII. Defendant knew or should have known their security systems were insufficient to protect the PII that is coveted by thieves worldwide. Defendant also failed to observe industry standard information security practices.

313. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

COUNT V
Invasion of Privacy
(On Behalf Of Plaintiffs And the Classes)

314. Plaintiffs hereby repeat and reallege paragraphs 1 through 244 of this Complaint and incorporate them by reference herein.

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

316. Defendant owed a duty to its current and former customers, employees, and its employees' dependents, including Plaintiffs and the Class Members, to keep this information confidential.

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

318. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and Class Members disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

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

321. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and

Class Members in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

322. Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

323. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

324. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

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

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

327. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class Members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT VI
Unjust Enrichment / Quasi Contract
(On Behalf Of Plaintiffs And the Classes)

328. Plaintiffs hereby repeat and reallege paragraphs 1 through 244 of this Complaint and incorporate them by reference herein.

329. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII. In so conferring this benefit, Plaintiffs and Class Members understood that part of the benefit Defendant derived from the PII would be applied to data security efforts to safeguard the PII.

330. Defendant appreciated that Plaintiffs and Class Members were conferring a benefit upon it and accepted that monetary benefit.

331. Acceptance of the benefit under the facts and circumstances described herein make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their 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.

332. 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.

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

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

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

336. 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 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 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.

337. 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.

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

COUNT VII
Violation of California's Unfair Competition Law (UCL)
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiffs Mejia, Huber and the California Subclass)

339. Plaintiffs hereby repeat and reallege paragraphs 1 through 244 of this Complaint and incorporate them by reference herein.

340. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

341. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), and other state data security laws.

342. Defendant stored the PII of Plaintiffs and the California Subclass in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff's and the California Subclass's PII secure to prevent the loss or misuse of that PII.

343. Defendant failed to disclose to Plaintiffs and the California Subclass that their PII was not secure. However, Plaintiffs and the California Subclass were entitled to assume, and did assume, that Defendant had secured their PII. At no time were Plaintiffs and the California Subclass on notice that their PII was not secure, which Defendant had a duty to disclose.

344. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and the California Subclass's nonencrypted and nonredacted PII.

345. Had Defendant complied with these requirements, Plaintiffs and the California

Subclass would not have suffered the injuries and damages related to the Data Breach.

346. Defendant's conduct was unlawful, in that it violated the CCPA.

347. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the Federal Trade Commission Act.

348. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

349. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

350. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

351. Instead, Defendant made the PII of Plaintiffs and the California Subclass accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiffs and the California Subclass to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under

the UCL because it violated the policies underlying the laws set out in the prior paragraph.

352. As a result of those unlawful and unfair business practices, Plaintiffs and the California Subclass suffered an injury-in-fact and have lost money or property.

353. For one, on information and belief, Plaintiffs' and the California Subclass's stolen PII has already been published—or will be published imminently—by cybercriminals on the dark web.

354. The injuries to Plaintiffs and the California Subclass greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

355. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

356. Therefore, Plaintiffs and the California Subclass are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT VIII
Violations of the California Consumer Privacy Act ("CCPA")
Cal. Civ. Code § 1798.150
(On Behalf of Plaintiffs Mejia, Huber and the California Subclass)

357. Plaintiffs hereby repeat and reallege paragraphs 1 through 244 of this Complaint and incorporate them by reference herein.

358. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiffs and the California Subclass. As a direct and proximate result, Plaintiffs and the California Subclass's nonencrypted and nonredacted

PII was subject to unauthorized access and exfiltration, theft, or disclosure.

359. Defendant is a "business" under the meaning of Civil Code § 1798.140 because Defendant is a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Civil Code § 1798.140(d).

360. Plaintiffs and California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiffs and California Subclass members' PII. Plaintiffs and California Subclass members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

361. Pursuant to California Civil Code § 1798.150(b), on February 21, 2024, Plaintiff Huber mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate.

362. On March 22, 2024, Defendant responded to Plaintiff Huber's CCPA notice letter claiming that Plaintiff had not provided any factual basis for a claim that Defendant violated the CCPA, that the Data Breach did not actually impact anyone's PII (it only "potentially" was impacted), and that Defendant "took steps to mitigate any potential risk to PII be commencing an investigation" and providing notification and complimentary credit monitoring to breach victims.

363. Additionally, Defendant did not respond to any of Plaintiff Huber's requests for information under California Civil Code sections 1798.100(a), 1798.110(a), 1798.115, and

1798.130(a)(2).

364. Pursuant to California Civil Code § 1798.150(b), on December 5, 2023, Plaintiff Mejia mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate.

365. On January 16, 2024, Defendant responded to Plaintiff Mejia's CCPA notice letter claiming that Plaintiff had not provided any factual basis for a claim that Defendant violated the CCPA, that the Data Breach did not actually impact anyone's PII (it only "potentially" was impacted), and that Defendant "took steps to mitigate any potential risk to PII be commencing an investigation" and providing notification and complimentary credit monitoring to breach victims.

366. Accordingly, because no cure is possible under these facts and circumstances, Plaintiff Huber and Plaintiff Mejia intend to seek statutory damages of between $100 and $750, in addition to all other relief afforded by the CCPA, including but not limited to equitable relief such as restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

367. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

368. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

COUNT IX
Violation of the California Consumer Records Act
Cal. Civ. Code § 1798.80, *et seq*.
(On Behalf of Plaintiffs Mejia, Huber and the California Subclass)

369. Plaintiffs hereby repeat and reallege paragraphs 1 through 244 of this Complaint and incorporate them by reference herein.

370. Under the California Consumer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, ***or*** is reasonably believed to have been, acquired by an unauthorized person." *Id* (emphasis added).

371. The Data Breach constitutes a "breach of the security system" of Defendant.

372. An unauthorized person acquired the personal, unencrypted information of Plaintiffs and the California Subclass.

373. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiffs and the California Subclass but waited approximately 254 days to notify them. Given the severity of the Data Breach, 254 days was an unreasonable delay.

374. Defendant's unreasonable delay prevented Plaintiffs and the California Subclass from taking appropriate measures from protecting themselves against harm.

375. Because Plaintiffs and the California Subclass were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier

notice.

376. Plaintiffs and the California Subclass are entitled to equitable relief and damages in an amount to be determined at trial.

COUNT X
Declaratory Judgment
(On Behalf of Plaintiffs and the Classes)

377. Plaintiffs hereby repeat and reallege paragraphs 1 through 244 of this Complaint and incorporate them by reference herein.

378. 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. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

379. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs and Class members continue to suffer injury from the ongoing threat of fraud and identity theft. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class members.

380. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

381. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

382. And if a second breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs and Class members' injuries.

383. If an injunction is not issued, the resulting hardship to Plaintiffs and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

384. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiffs, Class members, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Classes;

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

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. 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 patients, with additional training to be provided as appropriate based upon the patients' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information 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 patients' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing patients' 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; and

xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. 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.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Classes;

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

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

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

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

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

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: May 15, 2024

Respectfully Submitted,

By: *Raina C. Borrelli*

Raina C. Borrelli (*pro hac vice*)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109

Andrew J. Shamis, Esq.
Ohio Bar No. 100846
ashamis@shamisgentile.com
Leanna A. Loginov, Esq. (*pro hac vice*)

NY Bar No. 5894753
lloginov@shamisgentile.com
14 NE 1st Ave., Suite 705
Miami, Florida 33132
Telephone: 305-479-2299

LAUKAITIS LAW LLC
Kevin Laukaitis (*pro hac vice*)
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Christopher Weist
Ohio Bar No. Ohio 0077931
25 Town Center Blvd., Suite 104
Crestview, KY 41017
Tel: (513) 257-1895
Fax: (859) 495-0803
chris@cwiestlaw.com

Mason A. Barney
Tyler J. Bean
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com

Attorney for Plaintiffs and the Proposed Classes

CERTIFICATE OF SERVICE

I, Raina C. Borrelli, hereby certify that on May 15, 2024, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to counsel of record, below, via the ECF system.

DATED this 15th day of May, 2024.

STRAUSS BORRELLI PLLC

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
raina@straussborrelli.com
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109