Jason R. Hull (Utah 11202)
Anikka T. Hoidal (Utah 16489)
MARSHALL OLSON & HULL, PC
Ten Exchange Place, Suite 350
Salt Lake City, UT 84111
Tel: (801) 456-7655
jhull@mohtrial.com
ahoidal@mohtrial.com

*Pro Hac Vice Forthcoming

Attorneys for Plaintiff and Proposed Class

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

Thomas E. Loeser*
COTCHETT, PITRE & MCCARTHY, LLP
999 N. Northlake Way, Suite 215
Seattle, WA 98103
Tel: (206) 802-1272
tloeser@cpmlegal.com.com

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

Jennifer Keane, individually and on behalf of all others similarly situated,

Plaintiff,

v.

HealthEquity, Inc.,

Defendant.

CLASS ACTION COMPLAINT WITH JURY TRIAL

Case No. _____

TABLE OF CONTENTS

Page

Plaintiff Jennifer Keane, individually and on behalf of all others similarly situated ("Plaintiff"), brings this action against Defendant HealthEquity, Inc. ("Defendant"), seeking monetary damages, restitution, and/or injunctive relief for the proposed Class and Subclasses, as defined below. Plaintiff makes the following allegations upon information and belief, the investigation of counsel, and personal knowledge or facts that are a matter of public record.

INTRODUCTION

1. The release, disclosure, and publication of sensitive, private data can be devasting. Not only is it an intrusion of privacy and a loss of control, but it is a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.[1] A data breach can have a grave consequences for victims for years after the actual date of the breach—with the obtained information, thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain medical services, obtain government benefits, and/or obtain driver's licenses in the victims' names, forcing victims to maintain a constant vigilance over the potential misuse of their information.

2. Draper, Utah based HealthEquity markets itself as Health Saving Account Administrator with a mission to "save and improve lives by empowering healthcare consumers."[2]

3. On or about March 25, 2024, HealthEquity became aware of a systems anomaly requiring an extensive technical investigation and data forensics until June 10, 2024.[3]

[1] Dave Maxfield & Bill Latham, Data Breaches: Perspectives from Both Sides of the Wall, S.C. Lawyer (May 2014).
[2] https://www.healthequity.com/about (last visited on Aug. 1, 2024).
[3] Office of the Maine AG: Consumer Protection: Privacy, Identity Theft and Data Security Breaches (last visited Aug. 1, 2024)((Individual Notification Letter Template (3.29.2024)).

4. On June 26, 2024, Defendant admitted that it experienced a data breach in a Data Breach Notification Submission to the Office of the Maine Attorney General.[4] (the "Data Breach"). The Notification Submission states that the breach affected 4.3 million people.

5. What is extraordinarily troubling about the Data breach is that even though it knew how valuable customer information is, HealthEquity failed to adequately protect Plaintiff's and Class Members' Personal Identifiable Information ("PII"). This PII was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

6. HealthEquity has admitted that hackers gained access to protected health information and may have obtained the following: sign-up information for accounts and benefits including names, addresses, telephone numbers, employee IDs, employers, social security numbers, general contact information of dependents, and payment card information.[5]

7. As a result of the Data Breach, through which their PII and Personal Health Information ("PHI") was compromised, disclosed, and obtained by unauthorized third parties, Plaintiff and Class Members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud and identity theft for a period of years, if not decades. Furthermore, Plaintiff and Class Members must now and in the future closely monitor their

[4] *Id.*
[5] *Id.* (Individual Notification Letter Template (3.29.2024)).

financial accounts to guard against identity theft, at their own expense. Consequently, Plaintiff and the other Class Members will incur ongoing out-of-pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

8. By this Complaint, Plaintiff seeks to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

JURISDICTION, VENUE, AND CHOICE OF LAW

9. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1711, *et seq.*, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs. This Court also has diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a).

10. The Court has jurisdiction over HealthEquity, Inc. because HealthEquity, Inc. maintains its principal place of business in this District, has sufficient minimum contacts with this District, and has purposefully availed itself of the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District.

11. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because HealthEquity's principal place of business is located in this District and a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

PARTIES

A. Plaintiff Jennifer Keane

12. Plaintiff Jennifer Keane is a citizen of and is domiciled in the state of Washington.

13. Plaintiff is a customer of HealthEquity and has used its financial services for over 12 years.

14. Plaintiff provided confidential and sensitive PII and PHI to HealthEquity, as requested and required by HealthEquity for the provision of its services. HealthEquity obtained and continues to maintain Plaintiff's PII and PHI and has a legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

15. Plaintiff would not have entrusted her PII and PHI to HealthEquity had she known that HealthEquity failed to maintain adequate data security.

16. In light of her long association with HealthEquity and the description of those affected by the breach from HealthEquity's notice, Plaintiff believes that her that her information was compromised. Nonetheless, HealthEquity has yet to formally notify Plaintiff that it lost her PII and PHI.

17. Once she learned of the data breach, Plaintiff spent several hours taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect herself from data breaches, and reviewing her financial accounts for fraud or suspicious activity. She now plans to spend several hours a month checking account statements for irregularities.

18. As a result of the Data Breach, Plaintiff has suffered emotional distress from the release of her PII and PHI, which she expected HealthEquity to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using

her PII and PHI. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

B. Defendant

19. Defendant HealthEquity, Inc. is a Delaware corporation with its principal place of business in Draper, Utah. It is a Health Savings Account Administrator.[6]

20. In the course of its business, HealthEquity collects names, emails, physical addresses, social security numbers, dates of birth, phone numbers, names of dependents, names of authorized account users, technical information associated with the devices used by customers, and account transactions for payments to health care providers.[7]

FACTUAL BACKGROUND

A. HealthEquity Failed to Adequately Protect Customer Data, Resulting in the Data Breach

21. On the Privacy Notice page of its website, HealthEquity states: "Your privacy is important to us."[8] HealthEquity further claims to "honor all individual privacy rights defined by law, as set forth herein and in governing regulations."[9]

22. Notwithstanding these promises, on March 9, 2024, HealthEquity experienced a data breach affecting over 4.3 million people.[10]

23. HealthEquity claims to have discovered the data breach on June 26, 2024.[11] However, HealthEquity states in its Notice of Data Breach attached to its submission to the

[6] HealthEquity - Industry's #1 HSA Administrator (Aug. 1, 2024).
[7] General Privacy Notice | HealthEquity (Aug. 1, 2024).
[8] *Id.*
[9] *Id.*
[10] Office of the Maine AG: Consumer Protection: Privacy, Identity Theft and Data Security Breaches (last visited Aug. 1, 2024)(Individual Notification Letter Template (3.29.2024)).
[11] *Id.*

Maine Attorney General that it became aware there was a systems anomaly on March 25, 2024 and finished its data forensics and technical investigation in June 10, 2024.[12]

24. HealthEquity admitted its systems had been breached by hacking through a notice with the Office of the Maine Attorney General on July 26, 2024.[13]

25. HealthEquity was familiar with its obligations—created by contract, industry standards, common law, and representations to its customers—to protect customer information. Plaintiffs and Class Members provided their Private Information to HealthEquity with the reasonable expectation that HealthEquity would comply with its obligations to keep such information confidential and secure.

26. HealthEquity failed to comply with these obligations, resulting in the Data Breach. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records.

B. The Data Breach Puts Consumers at Increased Risk of Fraud and Identity Theft

27. An identity thief uses victims' PII, such as name, address, and other sensitive and confidential information, without permission, to commit fraud or other crimes that range from immigration fraud, obtaining a driver's license or identification card, obtaining government benefits, and filing fraudulent tax returns to obtain tax refunds.

28. Identity thieves can use a victim's PII to open new financial accounts, incur charges in the victim's name, take out loans in the victim's name, and incur charges on existing accounts of the victim. Plaintiffs' finances are now at risk due to the Data Breach.

[12] *Id.*
[13] *Id.*

29. Identity theft is the most common consequence of a data breach—it occurs to 65% of data breach victims.[14] Consumers lost more than $56 billion to identity theft and fraud in 2020, and over 75% of identity theft victims reported emotional distress.[15]

30. Plaintiff and members of the Class are now in the position of having to take steps to mitigate the damages caused by the Data Breach. Once use of compromised non-financial PII is detected, the emotional and economic consequences to the victims are significant. Studies done by the ID Theft Resource Center, a non-profit organization, found that victims of identity theft had marked increased fear for personal financial security. The report attributes this to more people having been victims before, contributing to greater awareness and understanding that they may suffer long term consequences from this type of crime.[16]

31. HealthEquity failed to protect and safeguard Plaintiff's and Class Members' private information, in fact failing to adhere to even its most basic obligations. As a result, Plaintiff and Class Members have suffered or will suffer actual injury, including loss of privacy, costs, and loss of time.

CLASS ACTION ALLEGATIONS

32. Plaintiff brings this action as a class action under Rule 23 of the Federal Rules of Civil Procedure, on behalf of a proposed nationwide class (the "Class"), defined as:

> All natural persons in the United States whose Personally Identifiable Information and/or Personal Health Information was compromised as a result of the Data Breach.

[14] Eugene Bekker, *What Are Your Odds of Getting Your Identity Stolen?*, IDENTITYFORCE (Apr. 15, 2021), https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics (last visited Feb. 1, 2023).
[15] *Id.*
[16] Identity Theft: The Aftermath 2013, Identity Theft Resource Center, https://idtheftinfo.org/latest-news/72 (last visited Feb. 1, 2023).

33. In addition, the State Subclasses are defined as follows:

> **Washington Subclass:** All natural persons in the State of Washington whose Personally Identifiable Information and/or Personal Health Information was compromised as a result of the Data Breach.

34. **Numerosity and Ascertainability:** Plaintiff does not know the exact size of the Class or identity of the Class Members, since such information is in the exclusive control of Defendant. Nevertheless, the Class encompasses at least 4.3 million individuals dispersed throughout the United States. The number of Class Members is so numerous that joinder of all Class Members is impracticable. The names, addresses, and phone numbers of Class Members are identifiable through documents maintained by Defendant.

35. **Commonality and Predominance:** This action involves common questions of law and fact which predominate over any question solely affecting individual Class Members. These common questions include:

a) whether Defendant engaged in the conduct alleged herein;

b) whether Defendant had a legal duty to use reasonable security measures to protect Plaintiff's and Class Members' PII and PHI;

c) whether Defendant timely, accurately, and adequately informed Plaintiff and Class Members that their PII and PHI had been compromised;

d) whether Defendant breached their legal duty by failing to protect the PII and PHI of Plaintiff and Class Members;

e) whether Defendant acted reasonably in securing the PII and PHI of Plaintiff and Class Members;

f) whether Plaintiff and Class Members are entitled to injunctive relief; and

g) whether Plaintiff and Class Members are entitled to damages and equitable relief.

36. **Typicality:** Plaintiff's claims are typical of the other Class Members' claims because all Class Members were comparably injured through Defendant's substantially uniform

misconduct, as described above. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other members of the Class that she represents, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and Class Members arise from the same operative facts and are based on the same legal theories.

37. **Adequacy:** Plaintiff is an adequate Class representative because her interests do not conflict with the interests of the other members of the Class she seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; and Plaintiff intends to prosecute this action vigorously. The Class's interest will be fairly and adequately protected by Plaintiff and her counsel.

38. **Superiority:** A class action is superior to any other available means 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. The damages and other detriment suffered by Plaintiff and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be virtually impossible for the Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not: individualized litigation creates a potential for inconsistent or contradictory judgments, increases the delay and expense to the parties, and increases the expense and burden to the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by this Court.

CAUSES OF ACTION

A. Claims Brought on Behalf of the Nationwide Class

COUNT ONE
NEGLIGENCE

39. Plaintiff incorporates all foregoing factual allegations as if fully set forth herein.

40. HealthEquity owed a duty to Plaintiff and Class Members, arising from the sensitivity of the information, the expectation the information was going to be kept private, and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, implementing, maintaining, monitoring, and testing HealthEquity's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' information was adequately secured from unauthorized access.

41. HealthEquity's Privacy Notice acknowledged HealthEquity's duty to adequately protect Plaintiff's and Class Members' PII and PHI.

42. HealthEquity's owed a duty to Plaintiff and Class Members to implement administrative, physical and technical safeguards, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiff's and Class Members' PII and PHI.

43. HealthEquity's also had a duty to only maintain PII and PHI that was needed to serve customer needs.

44. HealthEquity's owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and PHI.

45. HealthEquity's also had independent duties under Plaintiff's and Class Members' state laws that required HealthEquity to reasonably safeguard Plaintiff's and Class Members' PII and PHI, and promptly notify them about the Data Breach.

46. HealthEquity had a special relationship with Plaintiff and Class Members as a result of being entrusted with their PII and PHI, which provided an independent duty of care. Plaintiff's and Class Members' willingness to entrust HealthEquity with their PII and PHI was predicated on the understanding that HealthEquity would take adequate security precautions. Moreover, HealthEquity was capable of protecting its networks and systems, and the PII and PHI it stored on them, from unauthorized access.

47. HealthEquity breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Plaintiff's and Class Members' PII and PHI, including administrative, physical, and technical safeguards; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that its data security practices were inadequate to safeguard Plaintiff's and Class Members' PII and PHI.

48. But for HealthEquity's breach of its duties, including its duty to use reasonable care to protect and secure Plaintiff's and Class Members' PII, Plaintiff's and Class Members' PII and PHI would not have been accessed by unauthorized parties.

49. Plaintiff and Class Members were foreseeable victims of HealthEquity's inadequate data security practices. HealthEquity knew or should have known that a breach of its data security systems would cause damage to Plaintiff and Class Members.

50. It was reasonably foreseeable that the failure to reasonably protect and secure Plaintiff's and Class Members' PII and PHI would result in unauthorized access to

HealthEquity's networks, databases, and computers that stored or contained Plaintiff's and Class Members' PII and PHI.

51. As a result of HealthEquity's negligent failure to prevent the Data Breach, Plaintiff and Class Members suffered injury, which includes, but is not limited to, exposure to a heightened and imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiff and Class Members have also incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter and detect identity theft. The unauthorized acquisition of Plaintiff's and Class Members' PII and PHI has also diminished the value of the PII and PHI.

52. The harm to Plaintiff and Class Members was a proximate, reasonably foreseeable result of HealthEquity's breaches of its aforementioned duties.

53. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

COUNT TWO
NEGLIGENCE PER SE

54. Plaintiff incorporates all foregoing factual allegations as if fully set forth herein.

55. Under the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, HealthEquity had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII and PHI.

56. In addition, under state data security statutes, HealthEquity had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' PII and PHI.

57. HealthEquity breached its duties to Plaintiff and Class Members, under the Federal Trade Commission Act, 15 U.S.C. § 45, ("FTCA") and the state data security statutes, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

58. Plaintiff and Class Members were foreseeable victims of HealthEquity's violations of the FTCA and state data security statutes. HealthEquity knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiff's and Class Members' PII and PHI would cause damage to Plaintiff and Class Members.

59. HealthEquity's failure to comply with the applicable laws and regulations constitutes negligence *per se*.

60. But for HealthEquity's violation of the applicable laws and regulations, Plaintiff's and Class Members' PII and PHI would not have been accessed by unauthorized parties.

61. As a result of HealthEquity's failure to comply with applicable laws and regulations, Plaintiff and Class Members suffered injury, which includes but is not limited to the exposure to a heightened and imminent risk of fraud, identity theft, financial and other harm. Plaintiff and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiff and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class Members' PII and PHI has also diminished the value of the PII and PHI.

62. The harm to Plaintiff and the Class Members was a proximate, reasonably foreseeable result of HealthEquity's breaches of the applicable laws and regulations.

63. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

COUNT THREE
GROSS NEGLIGENCE

64. Plaintiff incorporates all foregoing factual allegations as if fully set forth herein.

65. Plaintiff and Class Members entrusted HealthEquity with highly sensitive and inherently personal private data subject to confidentiality laws.

66. In requiring, obtaining and storing Plaintiff's and Class Members' PII and PHI, HealthEquity owed a duty of reasonable care in safeguarding the PII and PHI.

67. HealthEquity's networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiff's and Class Members' PII and PHI were secured from unauthorized access.

68. HealthEquity's networks, systems, protocols, policies, procedures and practices, as described above, were not reasonable given the sensitivity of the Plaintiff's and Class Members' private data and the known vulnerabilities of HealthEquity's systems.

69. HealthEquity did not comply with state and federal laws and rules concerning the use and safekeeping of this private data.

70. Upon learning of the Data Breach, HealthEquity should have immediately disclosed the Data Breach to Plaintiff and Class Members, credit reporting agencies, the Internal Revenue Service, financial institutions and all other third parties with a right to know and the ability to mitigate harm to Plaintiff and Class Members as a result of the Data Breach.

71. Despite knowing its networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiff's and Class Members' PII and PHI were secured from unauthorized access, HealthEquity ignored the inadequacies and was oblivious to the risk of unauthorized access it had created.

72. HealthEquity's behavior establishes facts evidencing a reckless disregard for Plaintiff's and Class Members' rights.

73. HealthEquity, therefore, was grossly negligent.

74. HealthEquity's negligence also constitutes negligence per se.

75. The negligence is directly linked to injuries.

76. As a result of HealthEquity's reckless disregard for Plaintiff's and Class Members' rights by failing to secure their PII and PHI, despite knowing its networks, systems, protocols, policies, procedures and practices were not adequately designed, implemented, maintained, monitored and tested, Plaintiff and Class Members suffered injury, which includes but is not limited to the exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiff and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiff and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class Members' PII and PHI has also diminished the value of the PII and PHI.

77. The harm to Plaintiff and the Class Members was a proximate, reasonably foreseeable result of HealthEquity's breaches of the applicable laws and regulations.

78. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

COUNT FOUR
BREACH OF EXPRESS CONTRACTS

79. Plaintiff realleges and incorporate by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

80. Plaintiff and members of the Class, additionally and alternatively, allege that they entered into valid and enforceable express contracts with HealthEquity.

81. Under these express contracts, HealthEquity promised and was obligated to: (a) provide services to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII. In exchange, Plaintiff and members of the Class agreed to pay money for these services.

82. Both the provision of services, as well as the protection of Plaintiff's and Class Members' PII, were material aspects of these contracts.

83. HealthEquity's express representations, including, but not limited to, express representations found in HealthEquity's Privacy Notice, formed an express contract requiring HealthEquity to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII and PHI.

84. Alternatively, the express contracts included implied terms requiring HealthEquity to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII and PHI, including in accordance with federal, state and local laws, and industry standards.

85. Consumers value their privacy, the privacy of their dependents, and the ability to keep their PII and PHI associated with obtaining services private. To customers such as Plaintiff and Class Members, services that do not adhere to industry-standard data security protocols to protect PII and PHI are fundamentally less useful and less valuable than services that adhere to industry-standard data security. Plaintiff and Class Members would not have entered into these

contracts with HealthEquity without an understanding that their PII and PHI would be safeguarded and protected.

86. A meeting of the minds occurred, as Plaintiff and members of the Class provided their PII and PHI to HealthEquity and paid for the provided services in exchange for, amongst other things, protection of their PII and PHI.

87. HealthEquity materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Privacy Policy. Specifically, HealthEquity did not comply with federal, state and local laws, or industry standards, or otherwise protect Plaintiff's and the Class Members' PII and PHI, as set forth above. Further, on information and belief, HealthEquity has not yet provided Data Breach notifications to some affected Class Members who may already be victims of identity fraud or theft or are at imminent risk of becoming victims of identity theft or fraud associated with PII and PHI that they provided to HealthEquity. These Class Members are as yet unaware of the potential source for the compromise of their PII and PHI.

88. The Data Breach was a reasonably foreseeable consequence of HealthEquity's actions in breach of these contracts.

89. As a result of HealthEquity's failure to fulfill the data security protections promised in these contracts, Plaintiff and members of the Class did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in the contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in the value of the secure services they paid for and the services they received.

90. Had HealthEquity disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither Plaintiff, nor Class Members, nor any reasonable person would have purchased services from HealthEquity.

91. As a result of HealthEquity's breach, Plaintiff and Class Members suffered actual damages resulting from the theft of their PII and PHI, as well as the loss of control of their PII and PHI, and remain in imminent risk of suffering additional damages in the future.

92. As a result of HealthEquity's breach, Plaintiff and the Class Members have suffered actual damages resulting from their attempt to mitigate the effects of the breach of contract and subsequent Data Breach, including but not limited to, taking steps to protect themselves from the loss of their PII and PHI.

93. Accordingly, Plaintiff and the other members of the Class have been injured as a result of HealthEquity's breach of contracts and are entitled to damages and/or restitution in an amount to be determined at trial.

COUNT FIVE
BREACH OF IMPLIED CONTRACTS

94. Plaintiff incorporates all foregoing factual allegations as if fully set forth herein.

95. Plaintiff and Class Members were required to provide their PII and PHI to obtain services from HealthEquity. Plaintiff and Class Members entrusted their PII and PHI to HealthEquity in order to obtain services from them.

96. By providing their PII and PHI, and upon HealthEquity's acceptance of such information, Plaintiff and Class Members on one hand, and HealthEquity on the other hand, entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the services provided, whereby HealthEquity was obligated to take reasonable steps to secure and safeguard that information.

97. HealthEquity had an implied duty of good faith to ensure that the PII and PHI of Plaintiff and Class Members in its possession was only used in accordance with their contractual obligations.

98. HealthEquity was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiff's and Class Members' PII and PHI and to comply with industry standards and state laws and regulations for the security of this information, and HealthEquity expressly assented to these terms in its Privacy Policy as alleged above.

99. Under these implied contracts for data security, HealthEquity was further obligated to provide Plaintiff and all Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII and PHI.

100. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to HealthEquity, including paying for the services provided by HealthEquity and/or providing the PII and PHI required by HealthEquity.

101. HealthEquity breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII, resulting in the Data Breach. HealthEquity unreasonably interfered with the contract benefits owed to Plaintiff and Class Members.

102. Further, on information and belief, HealthEquity has not yet provided Data Breach notifications to some affected Class Members who may already be victims of identity fraud or theft, or are at imminent risk of becoming victims of identity theft or fraud, associated with the PII and PHI that they provided to HealthEquity. These Class Members are unaware of the potential source for the compromise of their PII and PHI.

103. The Data Breach was a reasonably foreseeable consequence of HealthEquity's actions in breach of these contracts.

104. As a result of HealthEquity's conduct, Plaintiff and Class Members did not receive the full benefit of the bargain, and instead received services that were of a diminished value as compared to the secure services they paid for. Plaintiff and Class Members, therefore,

were damaged in an amount at least equal to the difference in the value of the secure services they paid for and the services they received.

105. Neither Plaintiff, nor Class Members, nor any reasonable person would have provided their PII or PHI to HealthEquity had HealthEquity disclosed that its security was inadequate or that it did not adhere to industry-standard security measures.

106. As a result of HealthEquity's breach, Plaintiff and Class Members have suffered actual damages resulting from theft of their PII and PHI, as well as the loss of control of their PII and PHI, and remain in imminent risk of suffering additional damages in the future.

107. As a result of HealthEquity's breach, Plaintiff and the Class Members have suffered actual damages resulting from their attempt to mitigate the effect of the breach of implied contract and subsequent Data Breach, including, but not limited to, taking steps to protect themselves from the loss of their PII and PHI. As a result, Plaintiff and the Class Members have suffered actual identity theft and the ability to control their PII and PHI.

108. Accordingly, Plaintiff and Class Members have been injured as a result of HealthEquity's breach of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT SIX
BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING

109. Plaintiff realleges and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

110. Plaintiff and Class Members entered into and/or were the beneficiaries of contracts with Defendant, as alleged above.

111. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations—both explicit and fairly implied—and would not impair the rights of the other

parties to receive their rights, benefits, and reasonable expectations under the contracts. These included the covenants that Defendant would act fairly, reasonably, and in good faith in carrying out their contractual obligations to protect the confidentiality of Plaintiff's and Class Members' PII and PHI and to comply with industry standards and federal and state laws and regulations for the security of this information.

112. Special relationships exist between Defendant and Plaintiff and Class Members. Defendant entered into special relationships with Plaintiff and Class Members, who entrusted their confidential PII to Defendant and paid for services with Defendant.

113. Defendant promised and was obligated to protect the confidentiality of Plaintiff's and Class Members' PII and PHI from disclosure to unauthorized third parties. Defendant breached the covenant of good faith and fair dealing by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII and PHI, which resulted in the Data Breach. Defendant unreasonably interfered with the contract benefits owed to Plaintiff and Class Members by failing to implement reasonable and adequate security measures consistent with industry standards to protect and limit access to the PII and PHI of Plaintiff and the Class in Defendant's possession.

114. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant, including paying Defendant for services and providing it the confidential PII and PHI required by the contracts.

115. As a result of Defendant's breach of the implied covenant of good faith and fair dealing, Plaintiff and Class Members did not receive the full benefit of their bargain—services with reasonable data privacy—and instead received services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiff and Class Members have suffered actual damages in an amount equal to the difference in the

value between services with reasonable data privacy that Plaintiff and Class Members paid for, and the services they received without reasonable data privacy.

116. As a result of Defendant's breach of the implied covenant of good faith and fair dealing, Plaintiff and Class Members have suffered actual damages resulting from the theft of their PII and PHI and remain at imminent risk of suffering additional damages in the future.

117. As a result of Defendant's breach of the implied covenant of good faith and fair dealing, Plaintiff and Class Members have suffered actual damages resulting from their attempt to ameliorate the effect of the Data Breach, including, but not limited to, taking steps to protect themselves from the loss of their PII and PHI.

118. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class Members suffered injury in fact and are therefore entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Defendant from its conduct. Plaintiff also seeks reasonable attorneys' fees and costs under applicable law.

COUNT SEVEN
UNJUST ENRICHMENT
(ALTERNATIVE TO BREACH OF CONTRACT CLAIM)

119. Plaintiff realleges and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

120. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of monetary payments—directly or indirectly—for services received.

121. Defendant collected, maintained, and stored the PII and PHI of Plaintiff and Class Members and, as such, Defendant had knowledge of the monetary benefits conferred by Plaintiff and Class Members.

122. The money that Plaintiff and Class Members paid to Defendant should have been used to pay, at least in part, for the administrative costs and implementation of data management

and security. Defendant failed to implement—or adequately implement—practices, procedures, and programs to secure sensitive PII and PHI, as evidenced by the Data Breach.

123. As a result of Defendant's failure to implement security practices, procedures, and programs to secure sensitive PII and PHI, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in the value between services with reasonable data privacy that Plaintiff and Class Members paid for, and the services they received without reasonable data privacy.

124. Under principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members because Defendant failed to implement the data management and security measures that are mandated by industry standards and that Plaintiff and Class Members paid for.

125. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by Defendant. A constructive trust should be imposed upon all unlawful and inequitable sums received by Defendant traceable to Plaintiff and the Class.

COUNT EIGHT
DECLARATORY JUDGMENT

126. Plaintiff realleges and incorporates by reference the allegations contained in each of the preceding paragraphs as if fully set forth herein.

127. Plaintiff and the Class have stated claims against Defendant based on negligence, negligence per se, gross negligence and negligent misrepresentation, and violations of various state and federal statutes.

128. Defendant failed to fulfill its obligations to provide adequate and reasonable security measures for the PII and PHI of Plaintiff and the Class, as evidenced by the Data Breach.

129. As a result of the Data Breach, Defendant's system is more vulnerable to unauthorized access and requires more stringent measures to be taken to safeguard the PII and PHI of Plaintiff and the Class going forward.

130. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's current obligations to provide reasonable data security measures to protect the PII and PHI of Plaintiff and the Class. Defendant maintains that its security measures were—and still are— reasonably adequate and denies that it previously had or have any obligation to implement better safeguards to protect the PII and PHI of Plaintiff and the Class.

131. Plaintiff seeks a declaration that Defendant must implement specific additional, prudent industry security practices to provide reasonable protection and security to the PII and PHI of Plaintiff and the Class. Specifically, Plaintiff and the Class seek a declaration that Defendant's existing security measures do not comply with their obligations, and that Defendant must implement and maintain reasonable security measures on behalf of Plaintiff and the Class to comply with their data security obligations.

B. Claims Brought on Behalf of the Washington Subclass

COUNT NINE
WASHINGTON CONSUMER PROTECTION ACT
Wash. Rev. Code §§ 19.86.020, et seq.

132. Plaintiff, individually and on behalf of the Washington Subclass incorporates all foregoing factual allegations as if fully set forth herein. This claim is brought individually and on behalf of the Washington Subclass under the laws of Washington.

133. HealthEquity is a "person," as defined by Wash. Rev. Code § 19.86.010(1).

134. HealthEquity advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code § 19.86.010 (2).

135. HealthEquity engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Wash. Rev. Code § 19.86.020 including:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Washington Subclass Members' PII and PHI, which was a direct and proximate cause of the Data Breach;

b) Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Washington Subclass Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Washington Subclass Members' PII, including by implementing and maintain reasonable security measures;

e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Washington Subclass Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45.

f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Washington Subclass Members' PII and PHI; and

g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Washington Subclass Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45.

136. HealthEquity's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of HealthEquity's data security and ability to protect the confidentiality of consumers' PII and PHI.

137. Had HealthEquity disclosed to Plaintiff and Washington Subclass Members that its data systems were not secure and thus vulnerable to attack, HealthEquity would have been forced to adopt reasonable data security measures and comply with the law. HealthEquity was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Washington Subclass. HealthEquity accepted the responsibility of protecting the data, while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Washington Subclass Members acted reasonably in relying on HealthEquity's misrepresentations and omissions, the truth of which they could not have discovered.

138. HealthEquity acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and Washington Subclass Members' rights.

139. HealthEquity's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the many Washingtonians affected by the HealthEquity Data Breach.

140. As a direct and proximate result of HealthEquity's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Washington Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII;

overpayment for HealthEquity's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

141. Plaintiff and Washington Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

142. As a direct and proximate result of HealthEquity's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Washington Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; (iv) illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of PII and PHI; lost value of access to PII and PHI permitted by HealthEquity; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of HealthEquity's Data Breach; lost benefits of bargains as well as overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

143. Plaintiff and Washington Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, reasonable attorneys' fees and costs, and any other relief that is just and proper.

PRAYER FOR RELIEF

Plaintiff, on behalf of herself and on behalf of the proposed Class and Subclasses, request that the Court:

a. Certify this case as a class action, appoint Plaintiff as class representative, and appoint Plaintiff's Counsel as Class Counsel for Plaintiff to represent the Class;

b. Find that HealthEquity breached its duty to safeguard and protect the PII and PHI of Plaintiff and Class Members that was compromised in the Data Breach;

c. Award Plaintiff and Class Members appropriate relief, including actual and statutory damages, restitution and disgorgement;

d. Award equitable, injunctive and declaratory relief as may be appropriate;

e. Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

f. Award pre-judgment and post-judgment interest as prescribed by law; and

g. Grant additional legal or equitable relief as this Court may find just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand a trial by jury on all issues so triable.

Dated: August 6, 2024

Respectfully Submitted,

MARSHALL OLSON & HULL, P.C.

By: *Anikka T. Hoidal*
Jason R. Hull
Anikka T. Hoidal

COTCHETT PITRE & MCCARTHY LLP
Thomas E. Loeser (*Pro hac vice to be filed*)
Karin B. Swope
Ellen J Wen

MILBERG COLEMAN BRYSON PHILIPS GROSSMAN PLLC
Gary M. Klinger

Attorneys for Plaintiff and Proposed Class

ClassAction.org