UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

CASEY SIMPSON, on behalf of herself and all others Similarly situated, *Plaintiff*,	)	
	)	**CLASS ACTION COMPLAINT**
v.	)	
UKG INC., and KRONOS INCORPORATED, *Defendants.*	)	**JURY TRIAL DEMANDED**

Plaintiff, Casey Simpson ("Ms. Simpson"), on behalf of herself and all others similarly situated (the "Class" or "Class Members"), bring this action on behalf of themselves against Defendants UKG Inc. ("UKG") and Kronos Incorporated ("Kronos") (collectively, the "Defendants") to obtain damages, restitution and injunctive relief for the Class. Plaintiff alleges the following based on personal knowledge, the investigation of counsel, and information and belief.

NATURE OF THE ACTION

1. Plaintiff and Class Members provided their personally identifiable information ("PII") to MaineHealth, including names, addresses, employee IDs, and social security numbers, who in turn provided it to Defendants, who used the information to manage work schedules, track hours, and calculate paychecks. Due to Defendants' failure to implement and maintain reasonable safeguards to protect Plaintiff's PII it had been given, criminals obtained access to Plaintiff's PII, which resulted in substantial harm to Plaintiff and the Class.[1]

[1] *See UKG Kronos Community*, Communications Sent to Impacted Kronos Private Cloud (KPC) Customers, https://community.kronos.com/s/feed/0D54M00004wJKHiSAO?language=en_US.

2. This class action seeks to redress Defendant's negligent disclosure of over 8 million employees' PII in a massive data breach on or around December 11, 2021 ("Data Breach"). On that date, and possibly on others, Defendants inadequate security measures allowed unauthorized individuals to access and render unusable a workforce management software application MaineHealth used to process payroll and store data that contained the PII of Plaintiff and other individuals.[2]

3. As a result of the Data Breach, Plaintiff and the Class Members now bear an immediate and heightened risk of all manners of identity theft. Plaintiff and the Class Members have incurred and will continue to incur damages in the form of, *inter alia*, an imminent threat of identity theft, necessary mitigation expenses, loss of privacy and the value of personal information, deprivation of the benefit of the bargain, and/or the additional damages set forth in detail below.

JURISDICTION AND VENUE

4. This Court has personal jurisdiction over Defendant Kronos because it maintains a headquarters in and has its principal place of business in Massachusetts.

5. This Court has personal jurisdiction over Defendant UKG because it maintains a headquarters in Massachusetts.

6. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and Plaintiff and one or more members of the classes are residents of a different state from a defendant.

[2] *See id.*

7. Venue is proper in the District of Massachusetts because, pursuant to: (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to the claims occurred in Massachusetts, and (2) 28 U.S.C. § 1391(b)(1) in that Defendants are residents of Massachusetts.

PARTIES

8. Plaintiff Casey Simpson is a citizen of Springvale, Maine.

9. On approximately December 11, 2021, Plaintiff's PII was exposed in the Data Breach. If Plaintiff and the Class Members had known that Defendants would not adequately protect their PII, they would not have allowed Defendants access to this sensitive and private information.

10. Defendant UKG Inc. is a Delaware Corporation with a headquarters at 900 Chelmsford St., Lowell, MA 01851.

11. Defendant Kronos Incorporated is a Massachusetts Corporation with its principal place of business at 900 Chelmsford St., Lowell, MA 01851.

FACTUAL BACKGROUND

A. Plaintiff' and Class Members' Status As Employees

12. Plaintiff and Class Members were employed by MaineHealth during the relevant time period.

13. During the relevant time period, MaineHealth was a part of one of the largest health care systems in Maine and employed employees to work in numerous sectors of the health care industry.

B. Kronos' Data Breach.

14. Due to inadequate security measures, on or about December 11, 2021, Defendants were the subject of a ransomware attack, whereby criminals obtained access to Plaintiff's and Class Members PII, and Kronos Private Cloud was rendered unusable.[3]

15. Kronos Private Cloud is used by thousands of employers, including MaineHealth, and 8 million employees to manage work schedules, track hours, and calculate paychecks.[4]

16. Kronos stores employees' PII in Kronos Private Cloud, which can include, *inter alia*, employee names, addresses, employee ID numbers, and social security numbers.[5]

17. The PII of millions of individuals may have been exposed to unauthorized cybercriminals when they gained access to Kronos' server.[6]

18. By disclosing their PII to cybercriminals, Defendants put Plaintiff and all Class Members at risk of identity theft, financial fraud, and other serious harms.

19. Defendants negligently failed to take the necessary precautions required to safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure. Defendant's actions represent a flagrant disregard of Plaintiff's and the other Class Members' rights, both as to privacy and property.

C. Plaintiff's And Class Members' Personally Identifiable Information Is Valuable.

[3] *Id.*

[4] Becky Sullivan, *Hackers disrupt payroll for thousands of employers – including hospitals*, NPR (Jan. 15, 2022), https://www.npr.org/2022/01/15/1072846933/kronos-hack-lawsuits.

[5] Jennifer Korn, *Kronos ransomware attack could impact employee paychecks and timesheets for weeks*, CNN (Dec. 17, 2021), https://www.cnn.com/2021/12/16/tech/kronos-ransomware-attack/index.html.

[6] *See id.*

20. PII is of great value to hackers and cyber criminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners.

21. The term "personally identifiable information" refers to information that can be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and biometric records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[7]

22. Given the nature of this breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of different ways.

23. A study by Javelin Strategy and Research found that individuals lost about $13 billion in 2020 as a result of identity fraud.[8] Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

24. Indeed, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[9] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[10] Each of these fraudulent activities is difficult to detect. An individual may not know that their Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's

[7] *See* OFFICE OF MGMT. & BUDGET, OMBMEMORANDUM M-07-16 n. 1.
[8] *See Total Identify Fraud Losses Soar to $56 Billion in 2020*, BUSINESSWIRE (Mar. 23, 2021), https://www.businesswire.com/news/home/20210323005370/en/Total-Identity-Fraud-Losses-Soar-to-56-Billion-in-2020.
[9] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1, https://www.ssa.gov/pubs/EN-05-10064.pdf.
[10] *Id*. at 4.

employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

25. With access to an individual's PII, cyber criminals can do more than just empty a victim's bank account -- they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and social security number to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[11]

26. The cybercriminals who obtained Class Members' PII may also exploit the PII they obtained by selling the data in the so-called "dark markets." Having obtained these names, addresses, and Social Security numbers, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name.

27. In addition, if a Class Member's Social Security number is used to create a false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the employee's ability to gain employment or obtain a loan.

D. Defendants Were Aware of the Risk of Cyber-Attacks.

[11] *See Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft.

28. Data security breaches -- and data security breach litigation -- dominated the headlines in recent years, including in 2021.[12]

29. Defendants, being in the business of managing PII, were well aware of the risk of Cyber Attacks and the importance of keeping the information safe.

E. Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security and the Data Breach It Allowed.

30. Defendants represented to customers that they provided adequate security protections for their PII, and Class Members provided Defendants with sensitive personal information, including their Social Security numbers.

31. The cybercriminals will certainly use Class Members' PII, and Class Members will be at a heightened risk of identity theft for the rest of their lives. Plaintiff has incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of protecting their credit. By this action, Plaintiff and Class Members seek to hold Defendants responsible for the harm caused by their negligence.

32. In addition, as a direct and/or proximate result of Defendants' wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

33. Defendants' wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing

[12] *See e.g.*, Akanksha Rana, *T-Mobile Breach Hits 53 Million Customers as Probe Finds Wider Impact*, REUTERS (Aug. 20, 2021), https://www.reuters.com/technology/t-mobile-says-hackers-accessed-data-another-53-mln-subscribers-2021-08-20/; Jill McKeon, *St. Joseph's/Candler Suffers Ransomware Attack, EHR Downtime*, HEALTHITSECURITY (June 21, 2021), https://healthitsecurity.com/news/st-josephs-candler-suffers-ransomware-attack-ehr-downtime; David E. Sanger, Clifford Krauss, and Nicole Perlroth, *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES (May 8, 2021), https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.

increased risk of identity theft and identity fraud.[13] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[14] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[15] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. There is also a high probability that criminals who now possess Class Members' PII have not yet used the information but will do so at a later date or re-sell it.

34. The average cost per customer PII record was $180, based on a study by IBM and the Ponemon Institute.[16] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

35. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages, including, but not limited to, imminent threat of identity theft, necessary mitigation expenses, loss of privacy and the value of personal information, and deprivation of the benefit of the bargain.

F. Defendants' Response to the Data Breach Is Inadequate to Protect Class Members.

36. Defendants have failed to provide adequate compensation to Class Members harmed by its negligence. Defendants have not offered credit monitoring for those whose PII

[13] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267.
[14] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php.
[15] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, http://www.nclnet.org/datainsecurity_report.
[16] *See* Abi Tyas Tunggal, *What Is The Cost of a Data Breach in 2021?*, UPGUARD (Sept. 21, 2021), https://www.upguard.com/blog/cost-of-data-breach.

was stolen. Defendants have not offered Class Members any assistance in dealing with the IRS or state tax agencies. Nor have Defendants offered to reimburse Class Members for any costs incurred as a result of falsely filed tax returns, a likely consequence of the Data Breach.

CLASS ACTION ALLEGATIONS

37. Pursuant to Fed. R. Civ. P. 23, Plaintiff brings this action against Defendants as a class action on behalf of a Class of all individuals whose PII was compromised as a result of the Kronos Data Breach announced by Defendants on or about December 11, 2021 ("National Class").

38. Pursuant to Fed. R. Civ. P. 23, Plaintiff brings this action against Defendants as a class action on behalf of a Class of all employees of MaineHealth whose PII was compromised as a result of the Kronos Data Breach announced by Defendants on or about December 11, 2021 ("MaineHealth Class").

39. Plaintiff reserves the right to amend the above definition(s), or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

40. Excluded from the Class are Defendants; any parent, subsidiary, or affiliate of Defendants; any entity in which Defendants have or had a controlling interest, or which Defendants otherwise control or controlled; and any legal representative, predecessor, successor, or assignee of Defendants.

41. This action satisfies the requirements for a class action under F.R.C.P. 23(a)(1) - (a)(4), including requirements of numerosity, commonality, typicality, and adequacy of representation.

42. This action satisfies the requirements for a class action under Rule 23(a)(1). Plaintiff believes that the proposed Class as described above consists of more than 8 million employees that can be identified through Defendants' records, though the exact number and identities of Class Members are currently unknown. The Class is therefore so numerous that joinder of all members, whether otherwise required or permitted, is impracticable.

43. This action satisfies the requirements for a class action under Rule 23(a)(2). Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class Members. Common questions include, but are not limited to, the following:

a. Whether and to what extent Defendants had a duty to protect Class Members' PII;

b. Whether Defendants breached their duty to protect Class Members' PII;

c. Whether Defendants disclosed Class Members' PII;

d. Whether Defendants' conduct was negligent;

e. Whether Plaintiff and Class Members are entitled to damages; and

f. Whether Defendants' disclosure intruded upon the privacy of Plaintiff and Class Members.

44. This action satisfies the requirements for a class action under Rule 23(a)(3). The claims asserted by Plaintiff are typical of the claims of the members of the Class they seek to represent because, among other things, Plaintiff and Class Members sustained similar injuries as a result of Defendants' uniform wrongful conduct; Defendants owed the same duty to each class member; and Class Member's legal claims arise from the same conduct by Defendants.

45. This action satisfies the requirements for a class action under Rule 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests conflicting with the interests of Class Members.

46. Defendants have acted, or refused to act, on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or equitable relief with respect to the Class as a whole.

47. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because Class Members number in the hundreds or thousands and individual joinder is impracticable. Trial of Plaintiff's and Class Members' claims are manageable. Unless the Class is certified, Defendants will remain free to continue to engage in the wrongful conduct alleged herein without consequence.

48. The prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for Defendants.

49. Defendants' wrongful actions, inactions, and omissions are generally applicable to the Class as a whole and, therefore, Plaintiff also seeks equitable remedies for the Class.

50. Defendants' systemic policies and practices also make injunctive relief for the Class appropriate.

51. Absent a class action, Defendants will retain the benefits of its wrongdoing despite its serious violations of the law and infliction of economic damages, injury, and harm on Plaintiff and Class Members.

FIRST CAUSE OF ACTION

Against the Defendants On Behalf of The MaineHealth and National Class
(Negligence)

52. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

53. Defendants owed a duty to Plaintiff and to the Class to exercise reasonable care in obtaining, securing, safeguarding, properly disposing of and protecting Plaintiff and Class Member's sensitive information within its control from being compromised by or being accessed by unauthorized third parties. This duty included, among other things, maintaining adequate control over its computer systems and network so as to prevent unauthorized access thereof.

54. Defendants had full knowledge of the sensitivity of PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were compromised.

55. Defendants had a duty to exercise reasonable care to avoid foreseeable harm in its retention of Plaintiff's and Class Members' PII.

56. Defendants owed a duty of care to Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that its computer systems adequately protected the sensitive information of the patients in its facilities and networks.

57. Defendants breached their duty of care by failing to secure and safeguard the PII of Plaintiff and Class Members. Defendants failed to use reasonable measures to protect Class Members' PII. Defendants negligently stored and/or maintained its servers and systems.

58. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiff' and Class Members' PII would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members were reasonably foreseeable.

59. It was foreseeable that Defendants knew or should have known that its failure to exercise adequate care in safeguarding and protecting Plaintiff's and Class Members' PII would result in its release and disclosure to unauthorized third parties who, in turn, wrongfully used such PII or disseminated it for wrongful use.

60. Therefore, it was foreseeable to Defendants that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and Class Members: an imminent threat of identity theft, necessary mitigation expenses, loss of privacy and the value of personal information, deprivation of the benefit of the bargain, ongoing and imminent 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 confidentiality of the stolen confidential data; 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; and other economic and non-economic harm.

61. But for Defendants' negligent and wrongful breach of its responsibilities and duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

62. Had Defendants not failed to implement and maintain adequate security measures to protect the PII, Plaintiff's and Class Members' PII would not have been exposed to unauthorized access and they would not have suffered any harm.

63. As a direct and proximate result of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized release and

disclosure of PII, Plaintiff and Class Members have incurred, and will continue to incur, the above-referenced damages, and other actual injury and harm.

64. Defendants' wrongful actions, inactions, and omissions constituted (and continues to constitute) common law negligence.

65. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

SECOND CAUSE OF ACTION

Against the Defendants On Behalf of The MaineHealth Class and the National Class (Negligence Per Se)

66. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

67. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect sensitive personal identifying information.

68. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and failing to comply with industry standards. Defendants' conduct is particularly egregious and unreasonable because of the amount and nature of PII exposed.

69. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

70. Plaintiff's and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect. In addition, the harm that has occurred is the type of harm the FTC Act was intended to protect against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to maintain and employ reasonable security

measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Members of the Classes.

71. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have been injured as described above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION

Against Defendants On Behalf Of The National Class
(Violation of Materially Identical State Consumer Protection Statutes)

72. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

73. Plaintiff and Class Members' PII has been unlawfully exposed without their consent.

74. Defendants engaged in fraudulent or deceptive conduct that creates a likelihood of confusion or of misunderstanding.

75. Defendants knowingly misrepresented and intentionally omitted material information regarding the adequacy of their data security practices.

76. Despite knowledge that their data security measures were unreasonable and inappropriate, Defendants concealed the fact that employees' PII was not adequately secured.

77. Defendants acted deceptively by failing to inform Plaintiff and Class Members, who were required to disclose their PII as a condition of their employment, that their PII was not adequately secured.

78. Defendants' conduct directly, foreseeably and proximately caused Plaintiff and the National Class to suffer an ascertainable loss.

79. The practices discussed above all constitute unfair competition or unfair, unconscionable, deceptive, or unlawful acts or business practices in violation of at least the following state consumer protection statutes:

a. Alaska Unfair Trade Practices and Consumer Protection Act, Alaska Stat. § 45.50.471, *et seq.*;

b. Arizona Consumer Fraud Act, Ariz. Rev. Stat. Ann. § 44-1521, *et seq.*;

c. Colorado Consumer Protection Act, Colo. Rev. Stat. § 6-1-101, *et seq.*;

d. Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110a, *et seq.*;

e. Washington D.C. Code § 28-3901, *et seq.*;

f. Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, *et seq*.;

g. Kentucky Consumer Protection Act, Ky. Rev. Stat. Ann. § 367.110, *et seq*.;

h. Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.010, *et seq*.;

i. Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1601, *et seq*.;

j. New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 1358-A:1, *et seq.*;

k. New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-1, *et seq*.;

l. New York Deceptive Acts and Practices Act, N.Y. Gen. Bus. Law § 349, *et seq*.;

m. Ohio's Consumers Sales Practice Act, Ohio Revised Code § 1345.01, *et seq*.;

n. Oklahoma Consumer Protection Act, Okla. Stat. tit. 15, § 751, *et seq*.;

o. Rhode Island Unfair Trade Practices and Consumer Protection Act, R.I. Gen. Laws § 6-13.1-1, *et seq.*;

p. Vermont Consumer Fraud Act, Vt. Stat. Ann. Tit. 9 § 2451, *et seq.*; and

q. Washington Consumer Protection Act, Wash. Rev. Code § 19.86.010, *et seq*.

80. Plaintiff and Class Members are entitled to their actual damages and all other statutory and punitive damages available under these state consumer protection statutes.

81. Plaintiff and Class Members are further entitled to their costs and reasonable attorney fees.

82. Plaintiff and Class Members are also entitled to an order enjoining Defendant's unfair, unlawful, and deceptive practice, declaratory relief, and any other necessary or proper relief available under these state consumer protection statutes.

FOURTH CAUSE OF ACTION

Against Defendants On Behalf of The MaineHealth Class and the National Class (Intrusion Upon Seclusion/Invasion Of Privacy)

83. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

84. The Commonwealth of Massachusetts recognizes the right against "unreasonable, substantial or serious interference" with an individual's privacy. M.G.L.A. 214 § 1B.

85. Plaintiff and the Class Members had a reasonable expectation of privacy in the PII Defendants mishandled.

86. By failing to keep Plaintiff's and the Class Members' Private Information safe, and by recklessly misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants invaded Plaintiff's and Class Members' privacy by intrusion.

87. Defendants knew or should have known that ordinary persons in Plaintiff's or the Class Members' positions would consider Defendant's failure to carefully protect their data as

tantamount an intentional invasion of privacy; and Defendants' failure to guard the Plaintiffs' privacy, given the nature of its business, was highly offensive and objectionable.

88. Defendants invaded Plaintiff's and the Class Members' right to privacy and intruded into Plaintiff's and the Class Members' private affairs by conducting a cost benefit analysis that devalued the Plaintiff's and the Class Members' Private Information, without first obtaining their informed consent.

89. In failing to protect Plaintiff's and the Class Members' PII, and in recklessly misusing and/or disclosing their PII, Defendants' actions were tantamount to intentional malice and oppression; at minimunm, the Defendants acted with conscious disregard of Plaintiff's and the Class Members' rights to have such information kept confidential and private.

90. Plaintiff and the Class Members sustained damages (as outlined above) as a direct and proximate consequence of the invasion of their privacy by intrusion, and therefore seek an award of damages.

FIFTH CAUSE OF ACTION

Against Defendant On Behalf of The MaineHealth Class and the National Class (Declaratory and Injunctive Relief)

91. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

92. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

93. As previously alleged, Plaintiff and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII it collected from

Plaintiff and Class Members.

94. Defendants owed a duty of care to Plaintiff and Class Members requiring it to adequately secure their PII.

95. Defendants still possesses Plaintiff's and Class Members' PII.

96. Since the Data Breach, Defendants has announced few, if any, changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

97. Defendants have not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

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

99. There is no reason to believe that Defendants' security measures are any more adequate now than they were before the Data Breach to meet Defendants' legal duties.

100. Plaintiff, therefore, seeks a declaration (1) that Defendants' existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendants engages 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;

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

c. Ordering that Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

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

e. Ordering that Defendants' purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

f. Ordering that Defendants conducts regular computer system scanning and security checks;

g. Ordering that Defendants routinely and continually conducts internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendants to meaningfully educate its current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and the Class, respectfully request that the Court grant relief against Defendant as follows:

A. Certifying this class action pursuant to Rule 23 of the Federal Rules of Civil Procedure and requiring notice thereto to be paid by Defendants;

B. Appointing Plaintiff and their counsel to represent the Class;

C. For appropriate injunctive relief and/or declaratory relief, including an Order requiring Defendants to immediately secure and fully encrypt all confidential information, to properly secure computers containing confidential information, to cease negligently storing, handling, and securing its Employees' confidential information, and to provide identity theft monitoring for an additional five years;

D. Adjudging and decreeing that Defendants has engaged in the conduct alleged herein;

E. For compensatory and general damages according to proof on certain causes of action;

F. For reimbursement, restitution, and disgorgement on certain causes of action;

G.. For both pre- and post-judgment interest at the maximum allowable rate on any amounts awarded;

H. For costs of the proceedings herein;

I. For an Order awarding Plaintiff and the Class reasonable attorney's fees and expenses for the costs of this suit;

J. Trial by jury; and

K. For any and all such other and further relief that this Court may deem just and proper, including but not limited to punitive or exemplary damages.

Respectfully submitted,

June 16, 2022

Casey Simpson,
On behalf of Herself and Others
Similarly Situated, by Her attorney

/s/ Jonas A. Jacobson
Jonas A. Jacobson (BBO:676581)
2067 Massachusetts Ave., 5th Floor
Cambridge, MA 02140
617-230-2779
jonas@jonasjacobson.com