UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ROALD MARK, on behalf of himself and all others similarly situated, Plaintiff, v. SAMSUNG ELECTRONICS AMERICA, INC., Defendant.	Case No.: **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Roald Mark ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his undersigned counsel, brings this class action complaint against Defendant Samsung Electronics America, Inc. ("Samsung" or "Defendant"). Plaintiff alleges the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

NATURE OF THE ACTION

1. This is a class action brought on behalf of all persons who entrusted Samsung with sensitive personal information which was subsequently exposed in a data breach that was publicly disclosed by Samsung on September 2, 2022.[1]

2. In "late July" of 2022, hackers accessed Samsung's networks and servers and "acquired" its customers' sensitive personal information (the "Data Breach" or the "Breach").

[1] *Samsung Notification Letter*, SAMSUNG NEWSROOM U.S., https://news.samsung.com/us/notice-us-customer-information-cybersecurity/ (last visited September 15, 2022).

3. Defendant confirmed that the information breached included name, contact and demographic information, date of birth, and product registration information[2] ("personally identifiable information" or "PII").[3]

4. Samsung has not provided its customers with the exact dates as to when the breach occurred or how long it lasted.[4]

5. Samsung disclosed that it discovered customer information was "acquired" on August 4, 2022 as a part of an on-going investigation.[5]

6. The Data Breach was a result of Samsung's failure to properly secure and safeguard Plaintiff's and Class's sensitive personal information stored within its network and servers.

7. On September 2, 2022, Samsung began notifying affected individuals that their PII was compromised.[6] Samsung released its public announcement on the same day.

8. Samsung delayed alerting its customers about the Data Breach after discovering their information had been breached.

9. As of the date of this filing, it is unclear if Samsung has provided notice to all impacted individuals.

---

[2] *Id.*
[3] The definition of "demographic information" remains unclear; Samsung has not clarified even after reporting organizations requested that information. One tech publication believes it may include GPS location data. *See* Zack Whittaker, *Parsing Samsung's data breach notice*, TECHCRUNCH (Sept. 6, 2022, 1:00 PM EDT), https://techcrunch.com/2022/09/06/parsing-samsung-july-breach-notice/ (last visited September 15, 2022).
[4] *See* Zack Whittaker, *Parsing Samsung's data breach notice*, TECHCRUNCH (Sept. 6, 2022, 1:00 PM EDT), https://techcrunch.com/2022/09/06/parsing-samsung-july-breach-notice/ (last visited September 15, 2022).
[5] *Important Notice Regarding Customer Information*, SAMSUNG https://www.samsung.com/us/support/securityresponsecenter/ (last visited September 15, 2022).
[6] Attached hereto as Exhibit A is a copy of Plaintiff's notice letter he received via email.

10. When Samsung notified the public about the Data Breach, Samsung did not divulge pertinent information relating to the Breach, including the number of individuals affected and the categories of affected customers.[7]

11. Samsung claims that financial information and social security numbers were unaffected. Despite that claim, in its notice letter, Samsung informs the affected individuals that they are entitled to one free credit report annually from each of the three major nationwide credit reporting agencies.[8]

12. Defendant maintained the PII in a reckless and negligent manner. In particular, the PII was maintained on Defendant's network system in a condition vulnerable to cyberattacks.

13. Defendant exposed Plaintiff and Class Members to harm by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust network systems and security practices in place to safeguard its customers' PII; failing to take standard and reasonably available steps to prevent the Data Breach from occurring; failing to quickly detect the Data Breach; and failing to promptly notify Plaintiff and Class Members of the Data Breach.

14. Plaintiff and Class Members are now subject to ongoing and continuing risk of identity theft and fraud.

15. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a

[7] *See* Allen Bernard, *Impact of Samsung's most recent data breach unknown*, TECHREPUBLIC (Sept. 9, 2022, 1:04 PM PDT), https://www.techrepublic.com/article/samsung-data-breach/ (last visited September 15, 2022).
[8] *Important Notice Regarding Customer Information*, SAMSUNG, https://www.samsung.com/us/support/securityresponsecenter/ (last visited September 15, 2022).

billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action."[9]

16. Consumers who trusted Samsung to securely store their information have suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, out-of-pocket expenses, and value of time reasonably incurred to remedy or mitigate the effects of the data breach, loss of value of their personal information, and loss of the benefit of their bargain.

17. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party.

18. Plaintiff's claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of himself and all other similarly situated persons. Plaintiff seeks relief in this action individually and on behalf of a similarly situated class of individuals for negligence, breach of implied contract, invasion of privacy, and breach of confidence. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

[9] See Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last visited September 15, 2022).

PARTIES

19. Plaintiff Mark is a resident of Houston, Texas. On or around September 2, 2022, Plaintiff Mark received a notice of Data Breach letter from Samsung. Plaintiff Mark had shared his PII with Samsung to access services offered by Samsung. At or around the time he received the notice letter from Samsung, Plaintiff Mark began receiving communications from identity and privacy protection services. Plaintiff Mark suffered injury and was damaged as a result of Samsung's failure to keep his PII secure.

20. Defendant Samsung Electronics America, Inc., the designer, manufacturer, and vendor of electronics, is a corporation existing under the law of the State of New York and is headquartered at 85 Challenger Rd., Ridgefield Park, New Jersey 07660. Defendant Samsung regularly conducts business in this District and throughout the United States.

JURISDICTION AND VENUE

21. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class members; the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs; and at least one Class member is a citizen of a state different from Defendant.

22. This Court has personal jurisdiction over Defendant because Defendant is incorporated in New York.

23. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant is incorporated in this District and Defendant conducts substantial business operations in this District.

COMMON FACTUAL ALLEGATIONS

A. Samsung's Record Retention Services Are Advertised as Secure

24. Samsung was established in 1978 as a subsidiary of Samsung Electronics, to establish global brand awareness and provide its own service system.[10]

25. As a foreword to its specific privacy policies, Samsung outlines its general Privacy Principles.

26. In its Privacy Principles, Samsung notes that Transparency, Security, and Choice are the driving factors behind its Privacy Policy.[11]

27. Specifically, Samsung claims to "take data security very seriously. Our products are designed to keep your data private and secure . . . "[12]

28. Instead, Samsung obtains consumers' PII to complement its products and services, as outlined by the US Privacy Policy.[13]

29. According to the U.S. Privacy Policy, Samsung collects data to: 1) provide and enhance services, such as registering devices and identifying users; 2) providing targeted and generic ads; 3) communicating with users, including providing support; 4) turning user data into market research to improve Samsung's business; 5) identify and protect against criminal activity; and 6) comply with applicable legal requirements and enforce policies.[14]

---

[10] *History of Samsung Electronics (4): Innovation and efficiency combine for record-beating production and export boom! (1977~1978)*, SAMSUNG NEWSROOM (May 9, 2012), https://news.samsung.com/global/history-of-samsung-electronics-4-innovation-and-efficiency-combine-for-record-beating-production-and-export-boom-19771978 (last visited September 15, 2022).
[11] *Samsung's Privacy Principles,* SAMSUNG, https://www.samsung.com/us/privacy/ (last visited Sept. 15, 2022).
[12] *Id.*
[13] *Important Notice Regarding Customer Information*, SAMSUNG, https://www.samsung.com/us/support/securityresponsecenter/ (last visited September 15, 2022).
[14] *Samsung Privacy Policy for the U.S.*, SAMSUNG (last updated October 1, 2021), https://www.samsung.com/us/account/privacy-policy/#2 (last visited September 15, 2022).

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

31. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

32. Plaintiff and the 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.

B. Samsung's Data Systems Were Breached

33. In late July 2022, an unauthorized party acquired information from Samsung's systems.[15]

34. On August 4, 2022, Samsung "determined through [its] ongoing investigation that personal information of certain customers was affected."[16]

35. Samsung has not disclosed when those affected individuals were identified.[17]

36. On or around September 2, 2022, Samsung notified the public about the Data Breach.[18] Defendant announced that the PII included "information such as name, contact and demographic information, date of birth, and product registration information."

37. The same day Samsung publicly announced the Data Breach, Samsung also updated its privacy policy with a supplement.[19]

---

[15] *Important Notice Regarding Customer Information*, SAMSUNG, https://www.samsung.com/us/support/securityresponsecenter/ (last visited September 15, 2022).
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] Zack Whittaker, *Parsing Samsung's data breach notice*, TECHCRUNCH (Sept. 6, 2022, 1:00 PM PDT), https://techcrunch.com/2022/09/06/parsing-samsung-july-breach-notice/.

38. It is unclear exactly which data was acquired by hackers from the Data Breach based on Samsung's disclosures.

39. For example, Samsung stated that "demographic information" was acquired, which is not clearly defined in its U.S. Privacy Policy.

40. While demographic information is not clearly explained in the U.S. Privacy Policy or the Data Breach notice, Samsung pointed to its Ad Privacy Policy as a potential source of clarification of its demographic information sharing policies.[20]

41. The Ad Privacy Policy, effective January 1, 2020, claims that geolocation data may be collected for the purpose of serving "Customized Ads," among "other behavioral and demographic data."[21]

42. The Privacy Policy update, which supplements the previous privacy policy agreements, released on the day of the Data Breach announcement, changed the generic notice that demographic data used for customized ads into a notice that Samsung may track Samsung users' physical location via their devices, either as part of a security feature or to serve specific advertising for nearby Samsung or third-party stores, with separate consent.[22]

43. Samsung also added that it may store user content shared between users using the Quick Share feature,[23] which allows certain Galaxy devices to quickly share "photos, videos, and

---

[20] *Important Notice Regarding Customer Information*, SAMSUNG, https://www.samsung.com/us/support/securityresponsecenter/ (last visited September 15, 2022).
[21] *Samsung Ads Privacy Notice*, SAMSUNG, (January 1, 2020), https://www.samsung.com/us/account/privacy-policy/samsungads/ (last visited September 15, 2022).
[22] *Privacy Notice: Samsung account U.S. Privacy Notice*, SAMSUNG ACCOUNT (September 2, 2022), https://account.samsung.com/membership/policy/privacy (last visited September 15, 2022).
[23] *Id.* ("The Quick Share feature, available on certain Galaxy devices, enables you to quickly share photos, videos, and files. Quick Share can be used to share contents between Galaxy devices in close proximity to each other via the device-to-device method. Quick Share can also be used to share contents by sending a link that can be used to access the shared contents using any internet-connected device.").

files," for up to three days. Samsung provided no explanation as what content "files" refers to or may include.[24]

44. At this time, it is unclear whether Samsung has notified all of the affected consumers.

C. Samsung's Response Increased the Potential of Harm

45. As a result of Samsung's inability to secure Plaintiff's and Class's PII, Plaintiff and Class Members are now subject to the present and ongoing risk of identity theft, fraud, and other harm. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class Members.

46. Enhancing the danger to Plaintiff and the Class, Samsung was incapable of detecting the scope of the data breach for one to two weeks, at a minimum.

47. Because Samsung is silent as to when it detected the breach, Plaintiff and Class Members are unaware as to how long it took Samsung to determine their PII had been compromised.

48. At the Plaintiff's and Class's expense, it took weeks or months from the time Samsung discovered Plaintiff's and Class's PII had been exposed for Samsung to start notifying impacted consumers.

49. Samsung's efforts to ameliorate the damage it caused by failing to secure Plaintiff's and Class's PII included the suggestion that customers should make use of free credit reports.[25]

[24] *Id.*; Zack Whittaker, *Parsing Samsung's data breach notice*, TECHCRUNCH (Sept. 6, 2022, 1:00 PM EDT), https://techcrunch.com/2022/09/06/parsing-samsung-july-breach-notice/ (last visited September 15, 2022).
[25] Exhibit A.

CLASS ACTION ALLEGATIONS

50. Plaintiff brings this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Class:

> All persons who purchased or used Samsung products in the United States, and whose PII was compromised as a result of the July 2022 Data Breach (the "Class").

51. Plaintiff also brings this action individually and on behalf of the following Texas subclass:

> All persons who purchased or used Samsung products in the State of Texas, and whose PII was compromised as a result of the July 2022 Data Breach (the "Texas Subclass").

52. Specifically excluded from the Class are Samsung, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Samsung, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Samsung and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

53. Plaintiff reserves the right to amend the Class definition above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

54. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

55. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, Plaintiff estimates that the Class is

comprised of hundreds of thousands, or more, Class members. The Class is sufficiently numerous to warrant certification. The exact number of Class Members is in the possession and control of Defendant, and Defendant reported to the Attorney General of Maine that more than 1.5 million individuals were affected by the Data Breach.

56. Typicality of Claims (Rule 23(a)(3)): Plaintiff, like the other customers of Samsung, has been subjected to Samsung inadequate handling of their PII. Plaintiff is a member of the Class and his claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to that suffered by all other Class members that was caused by the same misconduct by Samsung.

57. Adequacy of Representation (Rule 23(a)(4)): Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

58. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class members is relatively small, the expense and burden of individual litigation make it impossible for individual Class members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Samsung will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

59. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class members present common questions of law or fact, which predominate over any questions affecting only individual Class members, including:

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

b. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendant's conduct was negligent;

d. Whether Defendant's conduct violated Plaintiff's and Class Members' privacy;

e. Whether Defendant took sufficient steps to secure its customers' PII;

f. The nature of relief, including damages and equitable relief, to which Plaintiff and members of the Class are entitled.

60. Information concerning Samsung's policies is available from Samsung's records.

61. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

62. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Samsung. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

63. Samsung has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

64. Given that Samsung has not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

65. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

66. Plaintiff brings this claim individually and on behalf of the Class members.

67. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

68. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

69. Defendant had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' PII within its possession was compromised and precisely the type(s) of information that were compromised.

70. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected its customers' PII.

71. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

72. 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 Private Information.

73. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII.

74. 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 its networks and systems;

c. Failure to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

75. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within Defendant's possession.

76. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

77. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

78. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff and Class Members' PII would result in injury to Plaintiff and Class Members. Further,

the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

79. It was foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII would result in injuries to Plaintiff and Class Members.

80. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

81. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

82. As a result of Defendant's failure to timely notify Plaintiff and Class Members that their PII had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

83. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

84. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

85. In connection with receiving services from Samsung, Plaintiff and all other Class members entered into implied contracts with Samsung.

86. Pursuant to these implied contracts, Plaintiff and Class members provided Samsung with their PII in order for Samsung to provide its services, for which Samsung is compensated. In exchange, Samsung agreed to, among other things, and Plaintiff understood that Samsung would: (1) provide services to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; and (3) protect Plaintiff's and Class members PII in compliance with federal and state laws and regulations and industry standards

87. In the ordinary course of providing its services, customers provide Defendant with PII.

88. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiff and Class members in its possession was secure.

89. Implied in these exchanges was a promise by Defendant to ensure the PII of Plaintiff and Class members in its possession was only used to provide the agreed-upon reasons, and that Defendant would take adequate measures to protect Plaintiff's and Class members' PII.

90. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiff's and Class members' PII to be accessed in the Data Breach.

91. Indeed, implicit in the agreement between Defendant and its customers was the obligation that both parties would maintain information confidentially and securely.

92. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiff and Class members would provide their PII in exchange for services by Defendant. These agreements were made by Plaintiff and Class members as customers of Defendant's.

93. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class members would not have disclosed their PII to Defendant but for the prospect of utilizing Defendant's services. Conversely, Defendant presumably would not have taken Plaintiff's and Class members' PII if it did not intend to provide Plaintiff and Class members with its services.

94. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosure and/or use.

95. Plaintiff and Class members accepted Defendant's offer of services and fully performed their obligations under the implied contract with Defendant by providing their PII, directly or indirectly, to Defendant, among other obligations.

96. Plaintiff and Class members would not have entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII.

97. Defendant breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' PII.

98. Defendant's failure to implement adequate measures to protect the PII of Plaintiff and Class members violated the purpose of the agreement between the parties.

99. Instead of spending adequate financial resources to safeguard Plaintiff's and Class

members' PII, which Plaintiff and Class members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiff and Class members.

100. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiff and Class members, Plaintiff and the Class members suffered damages as described in detail above.

COUNT III
INVASION OF PRIVACY
(On Behalf of Plaintiff and All Class Members)

101. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

102. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

103. Defendant owed a duty to Plaintiff and Class Members to keep their PII contained as a part thereof, confidential.

104. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and Class Members.

105. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and Class Members, by way of Defendant's failure to protect the PII.

106. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and Class Members is highly offensive to a reasonable person.

107. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as part of their relationships with Defendant in order to receive services from Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

108. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Member's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

109. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

110. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

111. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

112. Unless enjoined, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class

Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT IV
INVASION OF CONFIDENCE
(On Behalf of Plaintiff and All Class Members)

113. The preceding factual statements and allegations are incorporated by reference.

114. At all times during Plaintiff's and the Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Class's PII that Plaintiff and the Class entrusted to Defendant.

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

116. Plaintiff and the Class entrusted Defendant with their PII with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

117. Plaintiff and the Class also entrusted Defendant with their PII the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

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

119. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and the Class's PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Class's confidence, and without their express permission.

120. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class have suffered damages.

121. But for Defendant's disclosure of Plaintiff's and the Class's 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 Plaintiff's and the Class's PII as well as the resulting damages.

122. The injury and harm Plaintiff and the Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Class's PII. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Class's PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Class's PII.

123. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Class, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) 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, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate

and adequate measures to protect the PII of current and former patients and their beneficiaries and dependents; and (viii) present and 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 Plaintiff and Class members.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and his counsel as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) An award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury of all issues so triable.

Dated: September 19, 2022

LEVI & KORSINSKY, LLP

By: */s/ Mark S. Reich*

Mark S. Reich
Courtney E. Maccarone
55 Broadway, 10th Floor
New York, NY 10006
Telephone: 212-363-7500
Facsimile: 212-363-7171
Email: mreich@zlk.com
Email: cmaccarone@zlk.com

Counsel for Plaintiff