UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

MICHAEL BECKHAM, individually and on behalf of all others similarly situated, Plaintiff, v. SUNO, INC., Defendant.	CIVIL ACTION NO. 1:26-cv-14065 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Michael Beckham ("Plaintiff") brings this Class Action Complaint on behalf of himself, and on behalf of all others similarly situated, against Defendant Suno, Inc. ("Suno" or "Defendant"). The allegations concerning Plaintiff are based on his personal knowledge. The remaining allegations are based on counsel's investigation and information reasonably available before discovery, and are pleaded on information and belief where so stated.

NATURE OF THE ACTION

1. This action arises from a cybersecurity incident that occurred in or about November 2025 and resulted in the unauthorized acquisition and later circulation of personal information associated with more than 55 million Suno users (the "Data Breach").

2. Suno operates a generative artificial-intelligence music platform through which users create accounts, submit prompts and other content, generate music, and, in some instances, purchase subscriptions. To create and administer those accounts, Suno collects and maintains

personal information, including email addresses and account identifiers, and for some users' phone numbers, names, physical addresses, purchase information, and partial payment-card data.

3. Have I Been Pwned ("HIBP"), a widely used breach-notification service that obtained and analyzed the breached dataset, reports that the Data Breach included approximately 55.3 million unique email addresses; phone numbers where used as the sign-up method; and tens of thousands of Stripe purchase records containing names, physical addresses, purchase amounts, card type, expiration date, and the last four digits of payment cards. *See* Have I Been Pwned, "Suno Data Breach" (added July 20, 2026).[1]

4. Public reporting states that Suno confirmed a November 2025 security incident, did not dispute the reported scale, and had not publicly disclosed the incident or produced evidence of individualized user notice as of July 21, 2026.[2]

5. Plaintiff created a Suno account no later than the summer of 2024.

6. HIBP identifies Plaintiff's Suno account email address as included in the Suno breach corpus.

7. Following the Data Breach, Plaintiff experienced an increase in unsolicited spam telephone calls and phishing attempts. He has spent approximately ten hours investigating the incident, attempting to protect his other online accounts, reviewing and strengthening account security, monitoring for misuse, and consulting counsel regarding protective measures and his legal rights.

[1] Suno Data Breach, Have I Been Pwned, https://haveibeenpwned.com/Breach/Suno (last accessed July 22, 2026).

[2] Zack Wittaker, AI music generator Suno breach affects 55M users, per Have I Been Pwned, Tech Crunch (July 21, 2026), https://techcrunch.com/2026/07/21/ai-music-generator-sunobreach-affects-55m-users-per-have-i-been-pwned/.

8. Plaintiff's mitigation time is a present injury. His increased spam and phishing are also consistent with misuse of fresh account and contact data obtained through a targeted cyberattack. Suno's failure to provide Plaintiff a data-specific notice has made it more difficult and time-consuming for him to determine which accounts and communications require heightened scrutiny.

9. Plaintiff brings claims for negligence, breach of implied contract, breach of the implied covenant of good faith and fair dealing, unjust enrichment, and declaratory and equitable relief. He seeks damages for his lost time and other injuries, restitution and disgorgement where available, complete notice of the information affected, appropriate protective services, and reasonable prospective security and data-retention relief.

10. Suno may contend that online terms govern Plaintiff's claims. Plaintiff does not concede that Suno provided reasonably conspicuous notice of any arbitration agreement, class waiver, delegation clause, limitation period, liability cap, or other disputed term, or that he unambiguously assented to any such provision. Plaintiff pleads an implied contract and other claims without admitting the formation, scope, or enforceability of any purported online terms.

PARTIES

11. Plaintiff Michael Beckham is an adult domiciled in Huron, South Dakota.

12. Plaintiff is a Suno user whose account email address appears in the HIBP-verified Suno breach corpus. Plaintiff entrusted Suno with at least his email address and account information for the purpose of creating and maintaining his Suno account.

13. Defendant Suno, Inc. is a Delaware corporation with its principal place of business at 17 Dunster Street, Cambridge, Massachusetts 02138. Suno owns and operates the Suno generative-AI music platform, including suno.com and associated applications.

JURISDICTION AND VENUE

14. This Court has subject-matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d).

15. The proposed Class contains well over 100 members. HIBP reports approximately 55.3 million affected accounts worldwide, and the number of affected United States residents is readily expected to exceed 100.

16. Minimal diversity exists because Plaintiff is a citizen of South Dakota, while Suno is a citizen of Delaware, where it is incorporated, and Massachusetts, where it maintains its principal place of business.

17. The aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs, based on the size of the affected population, the value of Class Members' compensable time and other damages, restitutionary relief, protective services, and the cost and value of the requested equitable relief.

18. This Court has personal jurisdiction over Suno because Suno maintains its principal place of business in this District and the centralized conduct, omissions, security decisions, incident response, and notice decisions challenged in this action occurred in or emanated from Massachusetts.

19. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) and (b)(2) because Suno resides in this District and a substantial part of the events and omissions giving rise to Plaintiff's claims occurred here.

20. To the extent Suno contends that any forum-selection or governing-law provision applies, Suno's publicly available terms designate Massachusetts law and Massachusetts courts for

non-arbitrable disputes. Plaintiff does not concede assent to or enforceability of those terms, but Suno cannot reasonably dispute that this District is a proper and convenient forum.

RELATED ACTION

21. This action is related to *Pilavian v. Suno, Inc.*, No. 1:26-cv-13400 (D. Mass.), filed on July 24, 2026, because both actions arise from the same November 2025 Data Breach and concern overlapping putative classes and common issues of fact and law.

22. Plaintiff will file the required related-case materials and anticipates that coordinated proceedings or consolidation will promote efficiency, avoid inconsistent rulings, and conserve judicial and party resources.

FACTUAL ALLEGATIONS

A. Suno's Account-Based Platform and Collection of Personal Information

23. Suno markets a platform that allows users to generate songs and other audio through text prompts and related inputs.

24. A user must establish or access an account to use significant features of the platform. Suno associates the account with an email address, a phone number, or a third-party single-sign-on provider and maintains account identifiers and activity records.

25. Suno's present Privacy Notice acknowledges that it collects "Contact Information," "User Account Information," "User Activity Information," and user content when users create or access accounts and use the platform. It further states that Suno uses such information to perform its contract with users, authenticate accounts, operate the service, communicate with users, market offerings, maintain and secure the service, and develop and improve its products.

26. Suno's present Privacy Notice also acknowledges that the categories it has collected and disclosed during the preceding twelve months include identifiers, information covered by the

California Customer Records statute, commercial information, internet or network activity, geolocation information, uploaded visual and audio information, inferences, and account-access credentials.

27. Suno receives a substantial business benefit from account creation and user participation. Registered-user counts, user growth, engagement, contactability, subscription conversion, platform activity, and the information associated with accounts are valuable business assets and metrics.

28. Users, including Plaintiff, provide personal information for the limited and understood purposes of creating and maintaining accounts, authenticating access, receiving service communications, and using Suno's platform—not for disclosure to hackers, criminals, data brokers, or other unauthorized third parties.

29. When Suno solicited, collected, and retained user information, it knew that users reasonably expected Suno to employ safeguards appropriate to the volume, nature, and foreseeable misuse of the information in its custody.

30. Suno also knew that account email addresses and related identifiers are valuable to threat actors because they enable targeted phishing, impersonation, account discovery, social engineering, and correlation with data from other sources.

31. For payment-related users, the combination of name, address, purchase history, card brand, expiration date, and last four digits further enables highly credible phishing and financial impersonation.

32. Suno controlled the architecture, vendors, access permissions, retention periods, monitoring, incident-response procedures, and notice process for the systems in which Class Members' Personal Information was stored or processed.

33. Suno was therefore in the best position to prevent unauthorized access, detect anomalous activity, contain an intrusion, preserve evidence, determine the fields affected, and notify users promptly.

B. The Data Breach

34. In or about November 2025, an unauthorized actor gained access to and exfiltrated a massive dataset associated with Suno's users and systems.

35. The incident was not a speculative exposure or a misplaced device. HIBP obtained a copy of the breached dataset and validated more than 55 million unique email addresses within it.

36. The dataset included email addresses and, where used as a sign-up method, phone numbers. A smaller but still substantial Stripe subset included names, physical addresses, purchase amounts, card type, expiration dates, and the last four digits of payment cards.

37. The reported dataset was sufficiently complete and authentic for HIBP to create a dedicated Suno breach entry and to match individual email addresses—including Plaintiff's—to the Suno corpus.

38. Public reporting describes the incident as a cyberattack in which a hacker stole the information. Suno later confirmed that it experienced a security incident in November 2025 and did not dispute the reported number of affected users.

39. The scale of the exfiltration supports a reasonable inference that the unauthorized actor obtained access to a centralized or broadly accessible data store, account system, backup, export, administrative interface, source repository, or another high-value environment.

40. The precise attack vector, dwell time, systems traversed, privileges obtained, data queried, files exported, and security controls bypassed are known principally to Suno and its forensic investigators and will be developed through discovery.

41. On information and belief, the Data Breach resulted from one or more deficiencies in Suno's security program, including inadequate access controls, privilege management, authentication, network or data segmentation, monitoring, logging, anomaly detection, secure configuration, vendor oversight, data minimization, retention, incident response, or employee training.

42. On information and belief, reasonable security measures proportionate to the sensitivity and scale of Suno's data environment would have prevented the unauthorized access, materially reduced the amount of data accessible, or detected and contained the intrusion before the actor could exfiltrate a corpus of this magnitude.

43. The unauthorized actor's criminal conduct was foreseeable. Consumer platforms that collect millions of account identifiers, contact records, activity data, and payment-linked records are common targets for cyberattacks and social-engineering schemes.

44. Suno's duty to use reasonable care was heightened by the scale of its user base, the persistence of email addresses and contact identifiers, and the ease with which those identifiers can be used for targeted phishing and cross-dataset correlation.

C. Suno's Delayed and Incomplete Disclosure

45. The Data Breach occurred in or about November 2025 but did not come to broad public attention until July 2026—approximately eight months later.

46. HIBP added the Suno breach to its service on July 20, 2026. Public reporting followed on July 21, 2026.

47. At that time, Suno had not publicly disclosed the cyberattack on its website, and public reporting stated that Suno had not notified affected individuals that their information had been taken.

48. When asked, Suno confirmed the November 2025 incident but did not provide the publication with any user communication demonstrating that affected users had received notice.

49. Suno has not publicly identified the date it first learned of the intrusion, the date it confirmed exfiltration, the date it determined the affected fields, the systems involved, the duration of unauthorized access, the number of United States residents affected, or the steps taken to prevent recurrence.

50. Suno has not provided Plaintiff with a data-specific disclosure identifying every field tied to his account that was accessed or exfiltrated, whether his phone number was present, whether login-integration or activity data were present, whether downstream copies exist, or whether the actor retained or distributed his record.

51. The absence of timely, complete, and individualized information impaired Plaintiff's ability to take targeted protective action. A person who knows only that an email address was exposed must protect a broader range of accounts and communications than a person who is promptly told the exact fields and systems involved.

52. Prompt notice would have allowed Plaintiff and Class Members to begin monitoring earlier, distinguish legitimate Suno communications from impersonation, change security settings, review linked accounts, and protect payment or contact information before the dataset became more widely available.

53. Suno's delayed and incomplete response increased the amount of mitigation time required and prolonged the period during which affected users were unable to make informed decisions about their information.

54. To the extent Suno contends that it lacked a statutory duty to notify particular users because of the fields associated with a given record, that contention does not eliminate Suno's independent common-law and contractual duties to use reasonable care, investigate promptly, and provide accurate information necessary to mitigate a known unauthorized acquisition.

D. Plaintiff's Suno Account, Confirmed Exposure, and Resulting Harm

55. Plaintiff created a Suno account using his Gmail address no later than the Summer of 2024.

56. After the Suno breach became public, Plaintiff searched HIBP using the same email address associated with his Suno account.

57. HIBP identified that address as included in the Suno breach corpus.

58. The Data Breach involved targeted theft and actual acquisition of Suno's user dataset, not merely a theoretical vulnerability. Plaintiff's account address was found in the obtained corpus itself.

59. After the Data Breach, Plaintiff began receiving an increased volume of unsolicited spam telephone calls and phishing attempts compared with the period before the incident.

60. The increase in phishing is consistent with the known criminal uses of breached email and account data: identifying a target's online relationships, crafting credible lures, prompting password resets, impersonating services, and inducing disclosure of additional information.

61. Suno's failure to disclose the specific fields associated with Plaintiff's record prevents him from determining whether the increased spam telephone calls reflect direct exposure of a phone number supplied to or linked with Suno, correlation of his email with other data, or another use of the stolen corpus.

62. Plaintiff has nevertheless had to treat the threat as real because HIBP confirmed that the exact email address Suno used for his account was in the Suno dataset and because no other HIBP breach is associated with that address.

63. Plaintiff has spent approximately ten hours responding to the Data Breach and its consequences.

64. His mitigation efforts have included researching the incident; reviewing the security of other online accounts; attempting to protect those accounts from phishing, impersonation, and unauthorized access; monitoring communications and account activity; evaluating whether further password, authentication, or account changes were required; and consulting counsel about protective and legal options.

65. Plaintiff would have used that time for work, household, family, or other productive and personal activities but for the Data Breach and Suno's delayed and incomplete disclosure.

66. Plaintiff expects to spend additional time monitoring and responding to suspicious communications because his email address is persistent, the breached corpus cannot be recalled, and Suno has not identified every field associated with his record or every recipient of the data.

67. Plaintiff has also suffered loss of privacy and loss of control over when, how, and by whom his account information is used.

68. Plaintiff faces a continuing risk of targeted phishing, account takeover attempts, impersonation, and fraud because unauthorized actors can retain, combine, and reuse email addresses and other account-linked information indefinitely.

69. These injuries are concrete and particularized. They are tied to Plaintiff's confirmed inclusion in a targeted Suno dataset, the temporal increase in spam and phishing, the absence of another HIBP-listed breach for his account address, and the time he actually spent mitigating the consequences.

E. Online Terms and Formation Evidence are Within Suno's Control

70. Suno may attempt to enforce an arbitration agreement, class waiver, delegation clause, liability cap, limitations period, or pre-dispute notice procedure found in one or more versions of online terms.

71. Plaintiff does not concede that any such provision became part of a contract with him.

72. The exact signup method Plaintiff used, the screen or screens presented, the placement and formatting of any hyperlink, whether an affirmative checkbox was required, the text adjacent to the signup button, the device viewport, any A/B test or interface variant, and the version of terms allegedly in effect are factual issues that require preservation and discovery.

73. Suno possesses or controls the best evidence of formation, including historical interface code and screenshots, versioned terms, deployment logs, clickstream records, consent telemetry, account-creation logs, single-sign-on records, and any record purporting to show assent.

74. Plaintiff's assertion of an implied contract based on the parties' exchange of account services and personal information is not an admission that he assented to every term Suno may later identify.

75. Plaintiff reserves all arguments concerning formation, reasonable notice, manifestation of assent, incorporation by reference, retroactive modification, delegation, unconscionability, waiver, severability, scope, statutory nonwaiver, and enforceability.

F. Suno Failed to Use Reasonable Security and Incident-Response Practices

76. Reasonable security for a platform holding tens of millions of account records requires a documented, risk-based security program proportionate to the sensitivity and scale of the data.

77. Such a program includes, as applicable, data inventory and minimization; secure authentication; least-privilege access; privileged-account controls; encryption or tokenization; network and data segmentation; secure development and configuration; vulnerability management; logging and anomaly detection; egress monitoring; vendor management; backup protection; incident-response planning; and periodic independent testing.

78. Reasonable practices also require retention limits so that data no longer needed for a legitimate business purpose is deleted, anonymized, or isolated rather than left indefinitely available to attackers.

79. Reasonable incident response requires prompt containment, preservation of evidence, determination of the affected population and fields, assessment of legal notice duties, and accurate communication to affected persons in time for them to mitigate.

80. The Federal Trade Commission has repeatedly advised businesses to know what personal information they maintain, keep only what they need, protect it with appropriate controls, monitor for unauthorized access and exfiltration, and respond quickly to security incidents. These principles inform the standard of reasonable care even though Plaintiff does not assert a private cause of action under the Federal Trade Commission Act.

81. Suno knew or should have known that a failure to implement these measures could expose users to phishing, impersonation, spam, account takeover, fraud, loss of privacy, and substantial mitigation burdens.

82. Suno breached its duties by allowing unauthorized access to and exfiltration of a dataset containing more than 55 million account email addresses and other information.

83. Suno further breached its duties by failing to detect, contain, investigate, or disclose the incident with sufficient speed and completeness to permit Plaintiff and Class Members to protect themselves effectively.

84. Suno's current statement that it has implemented "commercially reasonable security measures and safeguards" confirms that security is an expected and material part of its relationship with users; the Data Breach and delayed disclosure plausibly show that the measures in place at the relevant time were not reasonable or were not reasonably implemented.

85. Suno's failures were a substantial factor in causing the unauthorized acquisition of Plaintiff's and Class Members' information and the resulting loss of time, privacy, control, and security.

86. The unauthorized actor's conduct does not sever causation because cyberattack and misuse were the very risks that reasonable security and timely notice were required to prevent or mitigate.

G. The Harm Is Ongoing

87. Email addresses and account identifiers do not expire in the same manner as a payment card. Plaintiff continues to use his email address for online accounts and communications.

88. Once a breached dataset has been copied and circulated, Suno cannot ensure that every copy has been recovered or deleted.

89. Threat actors can retain the data, wait for public attention to subside, and use the information later in phishing, impersonation, credential-recovery, and fraud schemes.

90. The risk is amplified when stolen data identify the specific service relationship because an attacker can tailor a message to a user's known interest in or account with Suno.

91. Plaintiff must therefore continue to scrutinize communications and account activity, and may need to take further protective measures as Suno discloses additional facts or as misuse emerges.

92. Suno has not informed Plaintiff that all personal information associated with his account has been deleted, that all unauthorized access pathways have been remediated, that all downstream copies have been contained, or that an independent assessment has validated its remediation.

93. Complete individualized notice identifying the fields associated with Plaintiff's record would directly reduce his present informational and mitigation injury by allowing him to focus protective measures on the accounts and information actually affected.

94. Reasonable retention, deletion, and security relief would reduce the risk that any information Suno continues to maintain about Plaintiff will be exposed again.

CLASS ALLEGATIONS

95. Plaintiff brings this action under Federal Rule of Civil Procedure 23 on behalf of himself and the following proposed classes:

Nationwide Class: All persons in the United States whose email address or other personal information was included in the dataset obtained from Suno in connection with the November 2025 Data Breach.

Subclass: All South Dakota residents who are members of the Nationwide Class.

96. Plaintiff may amend or refine the class definitions, add state-specific subclasses, or seek certification of particular issues as discovery clarifies the affected population, data fields, governing law, and Suno's records.

97. Excluded from the Classes are Suno; its parents, subsidiaries, affiliates, officers, directors, and legal representatives; entities in which Suno has a controlling interest; the judges assigned to this action and their immediate families; and persons who validly and timely opt out of any certified Rule 23(b)(3) class.

98. Numerosity. The Classes are so numerous that joinder is impracticable. HIBP reports approximately 55.3 million affected accounts worldwide. The United States and South Dakota populations can be identified from Suno's account, billing, geolocation, and incident records and are readily expected to number far more than forty.

99. Ascertainability. Membership can be determined using objective criteria, including the breached corpus, HIBP match data, Suno account records, incident-response records, user contact information, billing-country and address data, and other electronic records.

100. Commonality. Common questions of law and fact include:

a. The nature, scope, timing and cause of the Data Breach;

b. The systems, vendors, repositories, and data fields affected;

c. Whether Suno used reasonable security, retention, monitoring and incident-response practices;

d. When Suno learned or should have learned of unauthorized access and exfiltration;

e. Whether Suno's investigation and notice were timely and adequate;

f. Whether Suno owed duties independent of any written contract;

g. Whether reasonable security and prompt notice were terms of the parties' implied contracts;

h. Whether Suno was unjustly enriched by retaining user and business benefits while avoiding reasonable security costs;

i. Whether the criminal attack was foreseeable and whether it breaks causation;

j. Whether Class Members suffered compensable loss of time, privacy, control, value, or benefit of the bargain;

k. Whether declaratory and equitable relief is appropriate; and

l. The measure and administration of classwide or subclass relief.

101. Typicality. Plaintiff's claims arise from the same Data Breach and uniform security, retention, investigation, and notice practices as the claims of other Class Members. Like them, his personal information was included in the Suno dataset, and he suffered mitigation time, loss of privacy and control, and increased exposure to phishing and misuse.

102. Adequacy. Plaintiff will fairly and adequately protect the interests of the Classes. His interests are aligned with the Classes, and he has retained counsel experienced in complex litigation, privacy, data-security, and class actions.

103. Predominance. Common questions concerning Suno's centralized conduct, the breach, security practices, investigation, disclosure, and classwide duties predominate over individual questions. Individual damages, if any, can be determined through common methodologies, records, claims processes, subclasses, or other manageable procedures.

104. Superiority. A class action is superior because the cost of litigating individual claims would exceed many Class Members' recoveries; separate actions would risk inconsistent

adjudications; Suno and the affected population are dispersed; and common proof can resolve the principal liability issues efficiently.

105. Rule 23(b)(2). Suno has acted or refused to act on grounds generally applicable to the Classes by maintaining common security, retention, investigation, and notice practices, making declaratory and injunctive relief appropriate for the Classes as a whole.

106. Rule 23(c)(4). In the alternative, certification of common issues—including the existence and breach of duties, reasonableness of Suno's security and response, foreseeability, and entitlement to declaratory relief—would materially advance the litigation.

107. Choice of Law and Subclasses. Suno's challenged decisions were centralized in Massachusetts, and Suno publicly invokes Massachusetts law for its user relationship. Plaintiff therefore pleads nationwide claims under Massachusetts law where appropriate. If the Court determines that another state's law governs particular members or claims, state-specific subclasses, including the South Dakota Subclass, provide a manageable alternative.

[Remainder of this page left blank.]

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE

(On Behalf of Plaintiff, the Nationwide Class, and the South Dakota Subclass)

108. Plaintiff incorporates the preceding allegations as though fully set forth herein.

109. Suno owed Plaintiff and Class Members a duty to exercise reasonable care in collecting, storing, using, retaining, transmitting, securing, and disposing of their Personal Information.

110. That duty arose independently of any contract because Suno created and controlled a foreseeable risk of physical-world and digital harm by assembling a large repository of account and contact information and placing it within systems exposed to cyberattack.

111. Suno also assumed a duty by voluntarily undertaking to collect and safeguard Personal Information for account administration, authentication, communication, security, and other business purposes.

112. Suno owed a duty to use security measures proportionate to the volume, sensitivity, persistence, and foreseeable misuse of the Personal Information in its custody.

113. Suno owed a duty to retain Personal Information only as long as reasonably necessary and to segregate, delete, anonymize, or otherwise protect information that no longer served a legitimate purpose.

114. Suno owed a duty to maintain a reasonable incident-response program, investigate unauthorized access promptly, identify affected persons and fields, contain the incident, and provide timely and accurate information necessary for mitigation.

115. Suno knew or should have known that threat actors target consumer platforms and use breached email addresses, phone numbers, account relationships, purchase data, and partial card data for phishing, impersonation, fraud, and account takeover.

116. Suno breached its duties by, among other things:

a. Failing to design, implement, and maintain a reasonable security program;

b. Failing to limit access to and segment high-volume user and payment-linked data;

c. Failing to use reasonable authentication, privilege, monitoring, logging, anomaly-detection, and exfiltration controls;

d. Failing to identify and remediate vulnerabilities or insecure configurations;

e. Failing to minimize, delete, or isolate information no longer reasonably necessary;

f. Failing to detect and contain the intrusion before a massive corpus was exfiltrated;

g. Failing to investigate and determine the affected population and fields promptly;

h. Failing to provide prompt, complete, and individualized notice or data-specific disclosure; and

i. Failing to provide reasonable protective services and remediation information.

117. The unauthorized actor's criminal conduct was foreseeable and does not constitute a superseding cause because preventing and mitigating cybercrime was the object of Suno's duties.

118. Suno's breaches were actual and proximate causes of the unauthorized acquisition of Plaintiff's and Class Members' information and the resulting mitigation burden and loss of privacy and control.

119. Plaintiff's injury is plausibly traceable to Suno because his exact Suno account email appears in the Suno breach corpus; HIBP identifies no other breach involving that address;

he experienced increased spam and phishing after the incident; and he spent actual time responding to the confirmed exposure.

120. Plaintiff and Class Members suffered damages including lost time and opportunity costs; invasion and loss of privacy; loss of control over Personal Information; costs of monitoring and protection; increased spam and phishing; anxiety and distress associated with confirmed exposure and misuse risk; diminished value or utility of Personal Information; and the continuing risk and burden created by the compromised corpus.

121. To the extent applicable law requires injury to property, Plaintiff and Class Members have property and possessory interests in the confidentiality, control, use, and economic value of their Personal Information and account data, and the unauthorized acquisition impaired those interests.

122. To the extent any jurisdiction limits recovery for purely economic loss, Plaintiff and Class Members also allege non-economic privacy injury, loss of control, and other harms arising from a duty independent of contract. Plaintiff further pleads the South Dakota Subclass under South Dakota law if Massachusetts law does not govern those members.

123. Plaintiff and Class Members are entitled to compensatory, consequential, nominal, and other damages; equitable relief; pre- and post-judgment interest; and such further relief as the Court permits.

COUNT II
BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff, the Nationwide Class, and the South Dakota Subclass)

124. Plaintiff incorporates the preceding allegations as though fully set forth herein.

125. Plaintiff and Class Members entered into implied contracts with Suno when Suno offered account-based platform services and users accepted by providing or causing the provision of account information and establishing accounts.

126. Plaintiff accepted Suno's offer by creating a Suno account and providing his account email address. Suno accepted his information, established the account, and associated a display name with it.

127. The parties exchanged consideration. Suno provided access to its platform; Plaintiff and Class Members supplied personal information, account creation, attention, participation, user-growth value, contactability, and opportunities for engagement and conversion to paid services.

128. Reasonable security was an implied and material term of the exchange. A user who provides account and contact information for authentication and service administration reasonably understands that the platform will not expose that information to unauthorized actors through unreasonable security practices.

129. Prompt and accurate disclosure of a known unauthorized acquisition was also an implied term because users cannot protect themselves without information uniquely controlled by Suno.

130. Suno's own privacy representations and course of dealing confirm that it collects account information to perform its contract, authenticate users, operate and secure the service, and communicate with users—not to disclose the information to unauthorized third parties.

131. Plaintiff and Class Members performed their obligations by providing account information and the benefits associated with account creation and participation.

132. Suno breached the implied contracts by failing to use reasonable security; allowing unauthorized acquisition of the information; failing to minimize and protect retained data; and failing to provide prompt, complete, individualized notice and remediation information.

133. Suno's breaches deprived Plaintiff and Class Members of the secure account administration and data handling for which they bargained.

134. As a direct and foreseeable result, Plaintiff and Class Members suffered lost time, loss of privacy and control, increased phishing and misuse risk, monitoring and protection burdens, and loss of the benefit of their bargains.

135. Plaintiff does not plead this count as an admission that he assented to any separate arbitration agreement, class waiver, delegation clause, liability cap, limitations period, or other disputed online term. The implied promises pleaded here arise from the exchange actually performed and, alternatively, from any enforceable privacy commitments Suno contends were incorporated into the parties' relationship.

136. Plaintiff and Class Members are entitled to actual, consequential, nominal, and benefit-of-the-bargain damages and appropriate equitable relief.

COUNT III
BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

(On Behalf of Plaintiff, the Nationwide Class, and the South Dakota Subclass)

137. Plaintiff incorporates the preceding allegations as though fully set forth herein.

138. Every contract under Massachusetts law, South Dakota law, and the laws of other relevant states includes a covenant that neither party will act in bad faith to destroy or injure the other party's right to receive the fruits of the contract.

139. Plaintiff and Class Members performed their obligations and conferred the agreed account, data, and participation benefits on Suno.

140. The central fruits of the parties' account relationship included functional access to Suno's service and reasonable protection and handling of the information required to administer that access.

141. Suno violated the covenant by retaining the benefits of millions of user relationships while failing to use reasonable security, failing to minimize and protect retained data, and withholding timely and complete information about the known unauthorized acquisition.

142. Suno's delayed and incomplete disclosure forced users to bear mitigation burdens that Suno could have reduced through prompt, accurate notice.

143. Suno's conduct frustrated the reasonable expectations of Plaintiff and Class Members and deprived them of the benefit of their bargain.

144. As a direct and foreseeable result, Plaintiff and Class Members suffered the injuries described above and are entitled to damages and other relief.

COUNT IV
UNJUST ENRICHMENT / RESTITUTION

(Pleaded in the Alternative on Behalf of Plaintiff, the Nationwide Class, and the South Dakota Subclass)

145. Plaintiff incorporates the preceding allegations as though fully set forth herein.

146. Plaintiff pleads this count in the alternative to his contract claims to the extent the Court determines that no enforceable contract governs the challenged conduct.

147. Plaintiff and Class Members conferred concrete benefits on Suno by creating accounts, providing contact and account information, increasing Suno's registered-user base and growth metrics, enabling communications and marketing, and creating opportunities for platform engagement and paid conversion.

148. Suno knowingly accepted and retained those benefits.

149. The benefits are more specific than the mere passive receipt of information. Account creation and retained user data support Suno's service operation, user acquisition, market positioning, communications, analytics, product development, and enterprise valuation.

150. Suno also retained money and economic benefit by avoiding expenditures reasonably necessary for data minimization, access controls, monitoring, incident response, prompt notice, and protective services.

151. It would be unjust for Suno to retain the full value of the user and cost-saving benefits while shifting to Plaintiff and Class Members the time, privacy, monitoring, and security costs caused by Suno's inadequate practices.

152. Plaintiff and Class Members did not confer those benefits gratuitously or with the understanding that Suno could retain them while exposing their account information through unreasonable security practices.

153. Plaintiff and Class Members lack an adequate remedy at law to the extent contract or tort damages do not capture the benefits unjustly retained by Suno.

154. Equity requires restitution, disgorgement, or imposition of a constructive trust measured by the portion of benefits attributable to the security and privacy obligations Suno failed to provide, without duplication of damages awarded on other claims.

COUNT V
DECLARATORY AND EQUITABLE RELIEF

(On Behalf of Plaintiff, the Nationwide Class, and the South Dakota Subclass)

155. Plaintiff incorporates the preceding allegations as though fully set forth herein.

156. An actual controversy exists concerning Suno's duties to secure, minimize, retain, investigate, and disclose information associated with Plaintiff's and Class Members' accounts.

157. Suno has not provided Plaintiff a complete, individualized account of the fields associated with his record that were accessed or exfiltrated, the systems involved, the duration of access, the persons or entities that received the information, or the remediation performed.

158. Suno has not informed Plaintiff that all information associated with his account has been deleted, that all unauthorized pathways have been remediated, or that an independent review has validated the adequacy of its current security and retention practices.

159. Plaintiff continues to suffer an informational and mitigation injury because the absence of data-specific disclosure prevents him from tailoring protective measures to the information actually affected.

160. Plaintiff also faces a continuing risk concerning any Personal Information Suno continues to retain about him in systems shown to be vulnerable to unauthorized acquisition.

161. Under 28 U.S.C. §§ 2201–2202 and the Court's equitable authority, Plaintiff seeks declarations that:

a. Suno owed duties to use reasonable security and retention practices for users' Personal Information;

b. Suno breached those duties in connection with the Data Breach and its response;

c. Suno must provide affected users complete and accurate information reasonably available about the fields and systems implicated; and

d. Suno must maintain security, retention, deletion, and incident-response practices consistent with applicable law and the reasonable-care obligations described herein.

162. Plaintiff further seeks narrowly tailored equitable relief requiring Suno to provide individualized incident disclosures; identify the categories of data affected; maintain a reasonable written security and retention program; obtain periodic independent security assessments;

remediate material deficiencies; delete or de-identify information no longer reasonably necessary; and provide appropriate identity, phishing, and account-protection services for a period determined by the Court.

163. The requested disclosure and deletion relief would directly redress Plaintiff's present injuries by reducing uncertainty, allowing focused mitigation, and reducing the risk associated with information Suno continues to maintain.

164. Plaintiff lacks an adequate remedy at law for the continuing informational injury, loss of control, and risk associated with retained data and undisclosed incident details.

165. The balance of hardships and public interest favor relief requiring Suno to do what reasonable data custodians are already expected to do: accurately inform affected persons, minimize unnecessary data, remediate known weaknesses, and maintain reasonable security.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Class, respectfully requests that the Court grant the following relief:

A. Certifying the Nationwide Class and South Dakota Subclass under Rule 23, or certifying appropriate subclasses or issues, and appointing Plaintiff as class representative and his counsel as class counsel;

B. Entering judgment that Suno is liable on the claims asserted;

C. Awarding actual, compensatory, consequential, nominal, and punitive or exemplary damages to the extent permitted by applicable law;

D. Awarding restitution, disgorgement, and other equitable monetary relief without duplication;

E. Declaring the parties' rights and Suno's duties concerning security, retention, incident response, and notice;

F. Ordering Suno to provide complete and accurate individualized notice of the Data Breach and the categories of information affected;

G. Ordering reasonable prospective security, independent-assessment, retention, minimization, deletion, and remediation measures;

H. Ordering Suno to provide appropriate identity-theft, phishing, and account-protection services for not less than five years or such other period as the Court determines;

I. Awarding reasonable attorneys' fees, litigation expenses, and costs as permitted by law and equitable doctrine;

J. Awarding pre-judgment and post-judgment interest; and

K. Granting such other and further relief as the Court deems just and proper.

JURY TRIAL DEMANDED

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

Dated: September 3, 2026

Respectfully submitted,

/s/ *Stephen. J. Teti*
Stephen J. Teti (BBO# 569332)
LOCKRIDGE GRINDAL NAUEN PLLP
265 Franklin Street, Suite 1702
Boston, MA 02110
Tel.: (617) 535-3763
sjteti@locklaw.com

Kate M. Baxter-Kauf (admission *pro hac vice* forthcoming)
Karen H. Riebel (admission *pro hac vice* forthcoming)
Jacob E. Lanthier (admission *pro hac vice* forthcoming)
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 612-339-0981
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com
jelanthier@locklaw.com

Attorneys for Plaintiff