Hall Attorneys
A Professional Corporation
www.hallattorneys.com

FOR IMMEDIATE RELEASE

Hall Attorneys Files Class Action Against Suno Over Reported Data Breach Involving More Than 55 Million Accounts

D. Mass. complaint alleges Suno failed to protect account, contact, purchase, and payment data and failed to provide timely individualized notice after a November 2025 cyberattack.

To read the complaint, go to: **www.hallattorneys.com/dockets/suno**

Austin, Texas - July 29, 2026 - Hall Attorneys, P.C. and co-counsel filed a putative class action on July 28, 2026 against Suno, Inc. in the United States District Court for the District of Massachusetts. The case, Rugnetta v. Suno, Inc., No. 1:26-cv-13433, alleges that Suno failed to use reasonable safeguards to protect account and payment-linked information and failed to provide timely, complete, and individualized notice after a November 2025 cybersecurity incident.

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. According to the complaint, Suno collected and maintained email addresses and account identifiers and, for some users, telephone numbers, names, physical addresses, purchase information, and partial payment-card data. The suit alleges that this information can be used for targeted phishing, impersonation, account discovery, social engineering, and financial fraud.

The complaint cites Have I Been Pwned, which reportedly obtained and analyzed the breached dataset and identified approximately 55.3 million unique email addresses, telephone numbers used as the sign-up method, and tens of thousands of Stripe purchase records containing names, physical addresses, purchase amounts, and other payment information. Public reporting cited in the complaint 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.

The suit alleges that Suno controlled the systems, vendors, access permissions, retention periods, monitoring, incident-response procedures, and notice process for the affected environment. It further alleges that the approximately eight-month gap between the November 2025 incident and broad public disclosure impaired users' ability to distinguish legitimate communications from impersonation, harden linked accounts, and take targeted protective measures before the data circulated more broadly.

"Users should not have to discover through a third-party breach database that information tied to their accounts was taken months earlier," said attorney Nicholas Hall. "Email addresses and purchase-linked data can be used to build convincing phishing and impersonation attacks, and delayed notice leaves users to defend themselves without knowing exactly what was exposed."

Attorney Advertising. The complaint contains allegations only; no findings have been made. Do not send confidential information unless through the secure email address.

The named plaintiff is a California resident who created a Suno account no later than November 1, 2024. The complaint alleges that Have I Been Pwned identifies the exact email address associated with his Suno account in the Suno breach corpus and identifies no other known breach involving that address. Following the Data Breach, plaintiff allegedly experienced increased unsolicited spam telephone calls and phishing attempts and spent approximately ten hours investigating the incident, strengthening other accounts, monitoring for misuse, and consulting counsel. Suno allegedly has not provided him a data-specific notice identifying every field tied to his account that was accessed or exfiltrated.

The lawsuit seeks to represent a Nationwide Class of United States residents whose email address or other personal information was included in the dataset obtained from Suno and a California Subclass. It asserts claims for negligence, breach of implied contract, breach of the implied covenant of good faith and fair dealing, unjust enrichment and restitution, and declaratory and equitable relief. The requested relief includes damages, restitution, complete individualized notice, independent security assessments, remediation of material deficiencies, data minimization and secure deletion, and reasonable identity-theft, phishing, and account-protection services for not less than five years.

“This case is based on confirmed inclusion in the stolen Suno dataset, not a theoretical vulnerability,” Hall said. “The lawsuit seeks compensation for time and other harm already incurred and concrete security, retention, and notification reforms to reduce the continuing risk.”

Hall Attorneys is seeking additional proposed class representatives who reside in the United States, particularly paid Suno users and Illinois residents. Current or former Suno users should contact the firm if Have I Been Pwned identified their email address, or if they experienced increased spam or phishing, suspicious logins or password-reset attempts, account takeover, identity theft, financial loss, monitoring expenses, or substantial time spent protecting accounts after November 2025. In an initial message, provide your state of residence, when you used Suno, whether you paid for a subscription, whether Have I Been Pwned identified your email, and a short description of any suspicious activity, expense, or lost time.

Hall Attorneys is separately investigating potential biometric-privacy claims for Illinois users who, before November 2025, uploaded or recorded their own vocals, created a Suno Persona, or used another feature that preserved or reused their voice.

If you used Suno.com, go to **www.hallattorneys.com/suno** or email nhall@hallattorneys.com.

Do not delete your Suno registration or welcome emails, Have I Been Pwned notice or screenshot, account and profile screenshots, subscription receipts, Stripe, Apple, or Google payment records, spam and phishing messages, telephone call logs, password-reset or unfamiliar-login alerts, credit-monitoring receipts, identity-theft complaints, original vocal recordings, generated tracks, Persona records, or records of the time and money you spent responding. Preserve everything and contact Hall Attorneys promptly.

---Attorney Nicholas Hall is with Hall Attorneys, a Texas-based law firm focused on complex litigation and can be found on X.com @nicholashall or www.hallattorneys.com.
Inquiries: nhall@hallattorneys.com.

Attorney Advertising. The complaint contains allegations only; no findings have been made. Do not send confidential information unless through the secure email address.