

Robocall Mitigation Program Description

Radius Communications Inc.

FRN: 0037761731 | RMD Filing: RMD0031587

Date of this Plan: August 26, 2026

I. Introduction and Purpose

This Robocall Mitigation Program Description (the "Plan") is submitted by Radius Communications Inc. ("Radius" or the "Company"), a Pennsylvania corporation with its principal place of business at 201 King of Prussia Road, Suite 650, Wayne, Pennsylvania 19087, in connection with its filing in the Federal Communications Commission's (the "Commission" or "FCC") Robocall Mitigation Database (the "RMD"), pursuant to 47 CFR § 64.6305.

The Company is a non-facilities-based voice service provider that originates voice traffic on behalf of its end-user customers through an underlying wholesale voice carrier. The Company is committed to combating illegal robocalls and takes affirmative, documented steps to avoid originating illegal robocall traffic. This Plan describes the Company's robocall mitigation program, the specific measures it has implemented to comply with the Commission's rules, and the compliance governance controls it has adopted to ensure ongoing compliance and responsiveness to the Commission.

II. Principals, Affiliates, Subsidiaries, and Parent Companies

The individual with a controlling ownership interest in, and ultimate responsibility for the operations of, the Company is:

Desmond Spencer, Principal and Chief Executive Officer, Radius Communications Inc., 201 King of Prussia Road, Suite 650, Wayne, Pennsylvania 19087. Mr. Spencer is the sole individual with a controlling ownership interest in the Company.

The Company operates under the following affiliated entity: Fastdial Inc. Mr. Spencer holds sole controlling ownership over this affiliated operation as well. The Company has no separate parent company.

III. Caller ID Authentication (STIR/SHAKEN) Status

The Company does not hold its own SHAKEN certificate and has not obtained a Service Provider Code (SPC) token from the STIR/SHAKEN Policy Administrator. The Company therefore does not itself perform STIR/SHAKEN caller ID authentication, and it does not certify complete or partial implementation of the STIR/SHAKEN framework on its own network.

The Company originates traffic through an underlying wholesale voice carrier, Bandwidth Inc. Caller ID authentication for traffic the Company originates is performed by that underlying carrier under the carrier's own certificate and Operating Company Number (OCN). Because the Company has not implemented STIR/SHAKEN in its own right and does not hold an OCN or SPC token, the Company is subject to the robocall mitigation program obligation of 47 CFR § 64.6305(a) and submits this Plan, which describes the reasonable steps the Company takes to avoid originating illegal robocall traffic on its network. The Company will promptly update its filing, including its STIR/SHAKEN attestation and OCN field, if it obtains its own SHAKEN certificate and SPC token in the future.

Basis for No STIR/SHAKEN Implementation Obligation. The Company is a non-facilities-based voice service provider that does not own, lease, or operate any IP network element, session border controller, or SIP signaling infrastructure capable of performing STIR/SHAKEN authentication. All voice traffic the Company originates is transmitted over the IP network of its underlying wholesale carrier, Bandwidth Inc., which alone controls the signaling infrastructure necessary to authenticate and attest calls. Because the Company lacks control over that infrastructure, it is unable to implement STIR/SHAKEN under 47 CFR § 64.6301, consistent with the exemption recognized in the First Caller ID Authentication Report and Order, 35 FCC Rcd 3247, 3260, para. 40 (2020), and reflected in the certification requirements of 47 CFR § 64.6305(d)(2)(i). This is also why the Company does not hold an Operating Company Number (OCN) or Service Provider Code (SPC) token — SPC token issuance requires an OCN, which is assigned to entities operating their own network or interconnection facilities, a status the

Company does not hold as a pure reseller of Bandwidth's underlying network. Authentication of Company-originated traffic is instead performed by Bandwidth under Bandwidth's own certificate and SPC token. Accordingly, the Company is subject to the reasonable-steps robocall mitigation program requirement of 47 CFR § 64.6305(a), as described in this Plan.

IV. Reasonable Steps to Avoid Originating Illegal Robocall Traffic

Consistent with 47 CFR § 64.6305(a) and (d), the Company takes the following specific reasonable steps to avoid originating illegal robocall traffic:

Customer Vetting and Know-Your-Customer (KYC). Before provisioning service, the Company verifies the identity and legitimacy of each prospective customer, including verification of legal entity name and business registration, physical business address, responsible contact person, and the intended use case and expected calling patterns for the service. The Company declines service to prospective customers whose intended use or history indicates a risk of illegal robocalling.

The Company does not use any third-party vendor for KYC verification or traffic/analytics monitoring. These functions are performed in-house by Company personnel using the Company's own customer vetting procedures and call detail record review.

Application to Existing Customers. The Company applies its KYC and vetting procedures on an ongoing, not solely onboarding, basis. Existing customers are re-verified on at least an annual basis, and additionally upon any material change in calling volume or pattern, or upon referral by the Commission, law enforcement, or the industry traceback consortium. Re-verification includes reconfirming the customer's continued legal entity status, contact information, and consistency of actual calling patterns with the customer's stated use case.

Contractual Prohibitions. The Company's customer agreements expressly prohibit the use of its service to originate unlawful calls, including calls that violate the Telephone Consumer Protection Act or the Truth in Caller ID Act, and prohibit the use of inaccurate or unauthorized calling party numbers. The agreements reserve to the Company the right to suspend or terminate service immediately for such use.

Accurate Calling Party Information and Upstream Authentication. As described in Section III, traffic the Company originates is authenticated by its underlying wholesale carrier under that carrier's certificate. The Company supports that authentication by presenting only calling party numbers that are assigned to, or that the Company has verified the customer is authorized to use, and by refusing to transmit calling numbers that a customer cannot demonstrate authority to use.

Traffic Monitoring and Analytics. The Company monitors call detail records and signaling data for patterns and volumes indicative of illegal robocall activity, including abnormally high call volumes, high-volume short-duration calling, low answer-seizure ratios, spoofed, invalid, unallocated or unassigned calling numbers, rapid calling-number rotation, and other anomalous traffic characteristics.

Investigation and Mitigation of Suspicious Traffic. Upon identifying suspicious or potentially illegal traffic, whether detected internally or reported by the Commission, law enforcement, the industry traceback consortium, or another provider, the Company promptly investigates the traffic and its source. Where the Company determines that a customer is originating illegal traffic, the Company blocks the offending traffic and suspends or terminates the customer's account, and it does not accept the same traffic under a different account or identity.

Recordkeeping. The Company retains customer verification records, call detail records, traceback correspondence, and records of investigations and enforcement actions taken against customers, and makes such records available to the Commission and law enforcement upon request.

V. Traceback Request Commitment

The Company commits to respond fully and within 24 hours to all traceback requests from the Commission, from law enforcement, and from the industry traceback consortium designated by the Commission (currently the USTelecom Industry Traceback Group), and to cooperate with such entities in identifying and stopping any illegal robocaller that uses the Company's service to originate calls. Traceback requests are directed to the dedicated, actively monitored contact identified in Section VIII.

VI. Cooperation Commitment

The Company will cooperate with the Commission, law enforcement, and the industry traceback consortium in investigating and taking action against illegal robocalling activity involving the Company's network, and will provide such information and assistance as is reasonably requested to identify and stop illegal robocallers.

VII. Prior Commission Enforcement Action and Compliance Remediation

Disclosure of Prior Action. The Company answers in the affirmative that it has been subject to a formal Commission, law enforcement, or regulatory agency action or investigation. The Company's prior RMD filing (RMD File No. RMD0009101) was removed from the Robocall Mitigation Database, effective immediately, by FCC Enforcement Bureau order (DA 25-737, released August 25, 2025), following a related order released August 6, 2025 (DA 25-694), for failure to timely update the Company's certifications and robocall mitigation plan by the Commission's February 26, 2024 compliance deadline.

Agencies Involved. The FCC's Enforcement Bureau and Wireline Competition Bureau. The underlying investigation was opened under File No. EB-TCD-24-00036891 and was subsequently reassigned File No. EB-TCD-25-00038590.

Chronology. The Company was first notified of the deficiency on March 29, 2024. A Show Cause Order was issued on December 10, 2024. Removal became effective immediately upon release of the August 25, 2025 order, and the Company's certification could not be refiled without Commission approval.

Outcome. The Commission's action was based solely on certification and filing deficiencies. No finding of illegal robocalling, spoofing, or other unlawful conduct by the Company was made in connection with this matter.

Remediation. The Company has identified the root causes of the removal and implemented the following corrective controls:

Monitored point of contact. The point-of-contact address previously on file was no longer actively monitored following a personnel transition, and Commission notices sent to that address went unread. The point of contact has been updated to an actively monitored address, and a direct telephone number is now provided, as set out in Section VIII.

Named responsible officer. The Company has designated its Principal and Chief Executive Officer as the officer accountable for robocall mitigation compliance, with a designated secondary compliance contact, so that no single point of failure exists.

Deadline and filing calendar. The Company now maintains a compliance calendar tracking RMD filing obligations, annual review of this Plan, and any Commission-imposed deadlines, with advance reminders, to prevent a recurrence of the missed February 26, 2024 update deadline.

Escalation. All correspondence received from the Commission, law enforcement, or the industry traceback consortium is escalated to the responsible officer for same-business-day review.

VIII. Contact Information for Traceback and Takedown Requests

Radius Communications Inc.

Attn: Compliance / Traceback

201 King of Prussia Road, Suite 650, Wayne, Pennsylvania 19087

Primary contact: Desmond Spencer, Principal & Chief Executive Officer

Telephone: (484) 367-5000

Email: spencer@radiuscomm.com (actively monitored)

Secondary contact: Rizyl Yapsangco, Compliance — rizyly@radiuscomm.com

IX. Certification

The undersigned, an officer of Radius Communications Inc. with authority to make this submission, certifies that the statements contained in this Robocall Mitigation Program Description are true and accurate to the best of his knowledge, information, and belief, and that the Company has implemented the robocall mitigation measures described herein.

Respectfully submitted,

/s/ Desmond Spencer

Desmond Spencer

Principal & Chief Executive Officer

Radius Communications Inc.

Dated: August 26, 2026