

Revin, Inc. — Robocall Mitigation Plan

June 2026

Purpose

As a provider in the national telephone ecosystem, Revin has a corporate interest and legal obligation to protect the operation of the national phone system and its customers. This Robocall Mitigation Plan documents the technical and operational measures that Revin utilizes to discourage and mitigate robocall activity on its network.

Revin operates as a VoIP-based AI voice platform that originates and processes calls over IP networks, serving the home services industry. Revin provides AI-powered voice agents that handle inbound and outbound calls on behalf of its customers. PSTN interconnection and numbering resources are provided through Revin's upstream carrier partner. Revin does not directly administer NANPA numbering resources.

Certification

In submitting this RMP with the FCC, Revin states that: (a) all the calls it originates, carries, or processes on its network are subject to this RMP. For purposes of this Plan, "originates" refers to VoIP calls initiated through the Revin platform, and "processes" refers to real-time audio handling and AI-generated voice responses. Revin does not function as a traditional intermediate or transit carrier; any PSTN termination is performed through interconnection with Revin's upstream carrier partner. (b) Its prior certification has not been removed by Commission action and (c) it has not been prohibited from filing in the Robocall Mitigation Database ("RMD") by the Commission. Revin's RMP, which has been uploaded into the RMD, reflects the "reasonable steps to mitigate illegal robocall traffic" and "a commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers that use its service to originate, carry, or process illegal robocalls." Revin states that during the past two years, it (and/or any entity for which Revin shares common ownership, management, directors, or control) has not been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging,

assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient RMD certification or mitigation program description.

Mitigation Measures

1. Customer Onboarding and Verification

Revin serves business customers in the home services industry. Revin does not offer any form of self-service signup. Every customer is manually onboarded by Revin personnel, who directly verify the customer's identity, business legitimacy, and operational use case before account provisioning. No account can originate calls without explicit Revin staff involvement in its setup. Revin therefore maintains a direct, documented relationship with every entity originating calls on its platform. Accounts requesting outbound call capacity are subject to additional review and ongoing monitoring.

2. Access Controls

Revin protects all of its services with infrastructure-level access controls. API access is authenticated and scoped to verified customer accounts. All platform services are deployed behind secure network boundaries with monitoring for unauthorized access attempts.

3. Rate Limiting and Call Controls

Outbound calling is restricted to configured campaigns and workflows tied to verified customer accounts. Call volume is governed by per-customer limits established during onboarding. Outbound calling activity is subject to monitoring for anomalous traffic patterns, and Revin may restrict, suspend, or terminate accounts exhibiting suspicious activity.

4. Monitoring and Threat Detection

Revin reviews call traffic and platform activity for anomalous patterns. Indicators of potential abuse — including unusual call volumes, unexpected geographic patterns, and other anomalies — are surfaced through ongoing review by Revin personnel, automated alerting on traffic indicators, and coordination with the upstream carrier's network-level monitoring. Any identified anomalies are promptly investigated and addressed.

5. Incident Response

Revin participates in and acts on reports from industry partners through coordination with its upstream carrier partner, which is a registered participant in the USTelecom Industry Traceback Group (ITG). Where applicable, call authentication and related network-level

controls are implemented in coordination with the upstream carrier. Reports of Acceptable Use Policy (AUP) violations, including suspected illegal robocalls, are reviewed and responded to within 24 hours. Such reports include those received from ITG (via the upstream carrier), the upstream carrier directly, customers, and other industry partners. Revin's contracts with its customers and upstream providers include AUP requirements subject to enforcement via monitoring and manual review, and Revin may suspend or terminate accounts engaged in suspected violations.

6. Third-Party Analytics

Revin does not contract with third-party telephony analytics vendors (such as outbound call reputation or spam-scoring services) for STIR/SHAKEN attestation, call rating, or analogous outbound telephony analytics. Revin does use third-party observability infrastructure for internal platform telemetry, alerting, and log aggregation. Outbound call traffic analysis and fraud detection are performed using these internal monitoring tools and in coordination with the upstream carrier's network-level controls.

7. Training

Revin maintains internal policies governing personnel responsibilities related to robocall mitigation, including customer onboarding requirements, traceback request handling, and AUP enforcement. Revin has implemented a structured training program covering illegal robocall concerns, traceback procedures, customer onboarding requirements, and applicable regulatory obligations. The program is required for all personnel involved in customer onboarding, account management, and platform operations, and is incorporated into Revin's personnel onboarding process.

8. Terms of Service

Revin's services enable AI-driven voice and messaging functionality for home services businesses. Revin's customer agreements (the Master Services Agreement and applicable Service Orders) contractually require each customer to comply with all applicable communications laws, including the Telephone Consumer Protection Act (TCPA), the CAN-SPAM Act, Canada's Anti-Spam Legislation (CASL), and the Canadian Radio-television and Telecommunications Commission (CRTC) Unsolicited Telecommunications Rules. Customers represent and warrant that all recipients of communications sent through the Platform have provided valid prior express consent as required by applicable law, agree to maintain consent and opt-out records for at least seven (7) years, and agree to forward any opt-out request to Revin within twenty-four (24) hours of receipt. Revin reserves the right to monitor platform activity, investigate suspected misconduct, and suspend or terminate accounts engaged in

unlawful robocall activity. Revin cooperates with upstream carriers and traceback entities in investigating and mitigating suspected violations.

Company, Principals, and Affiliates

Legal Company Name

Revin, Inc.

Principals

None

Affiliates

None

Employee Responsible for Addressing Robocall Mitigation

The following Revin employee is the designated point of contact for inquiries from the FCC, the USTelecom Industry Traceback Group (ITG), and law enforcement agencies:

Contact Name: Stephen Webel

Contact Title: Head of Engineering

Contact Business Address: 900 Broadway, Suite 1003, New York, New York, 10003

Contact Telephone: 207-272-9013

Contact Email: webel@revin.ai

Revision History

Description	Date
Initial filing	June 2026