

Robocall Mitigation Program

Entity Name: RadWeb, LLC

Filer Identification Number: 838274

Service Provider Type: Voice Service Provider (Hosted VoIP/Cloud Communications)

This document describes the reasonable steps taken by RadWeb (the "Company") to avoid originating illegal robocall traffic, and serves as our formal commitment to cooperating with traceback requests, in compliance with 47 CFR § 64.6305(d)(ii) and (iii).

Section 1: Specific, Reasonable Steps to Avoid Originating Illegal Robocalls (47 CFR § 64.6305(d)(ii))

The Company employs a multi-layered approach to mitigate the risk of originating illegal robocall traffic. Our program integrates customer vetting, proactive monitoring, and a rigorous enforcement policy.

1.1. Customer Vetting and Know Your Customer (KYC) Procedures

- **New Customer Screening:** All new customers undergo a mandatory screening process that includes verifying business entity details, physical address, and primary contact information. High-volume traffic or bulk-calling customers are subject to enhanced due diligence.
- **AUP Requirement:** All customers must explicitly agree to the Company's Acceptable Use Policy (AUP), which strictly prohibits the use of the platform for illegal, unsolicited, or fraudulent telemarketing, including illegal robocalls and spoofing in violation of the TRACED Act and FCC rules.
- **High-Risk Traffic Review:** Before activation, any requested usage patterns indicating potential high-volume, short-duration (HVSD) traffic are flagged for manual review by the compliance team to confirm legitimate use cases (e.g., appointment reminders, emergency services).

1.2. Proactive Traffic Monitoring and Analytics

- **Real-time Call Monitoring:** The Company utilizes an automated system to monitor originating call traffic for specific signatures commonly associated with illegal robocalls, including:
 - **High Call Completion Ratio (CCR) to Low Call Duration:** A high number of calls with very short or zero duration, suggesting rapid dialing, which is common in "shotgun" campaigns.

- **High Call Attempts Per Second (CAPS):** Traffic volumes significantly exceeding established or legitimate baselines for the customer's profile.
- **Sequential Number Dialing:** Detection of rapid, consecutive calls to sequential blocks of numbers, indicative of list churning or war-dialing.
- **Reporting and Alerting:** Automated alerts are generated for any customer whose traffic exceeds predefined volume and pattern thresholds, immediately escalating the account for internal investigation.
- **Number Spoofing Check:** We verify that customers using a non-Company-provided Caller ID have the right to use that number (Known Customer-Assigned Numbers) and monitor for evidence of unauthorized or dynamically changing spoofed Caller ID information.

1.3. Remedial and Enforcement Policy

- **Initial Investigation:** Upon receiving a monitoring alert or a formal complaint (e.g., from the Industry Traceback Group or other providers), the Company's compliance team conducts an immediate investigation of the customer's traffic.
- **Warning and Remediation:** If evidence suggests a violation of the AUP or potential illegal activity, the customer is issued a formal warning requiring immediate cessation of the problematic traffic and a written remediation plan.
- **Immediate Suspension and Termination:** The Company reserves the right, and is committed, to immediately suspending service without prior notice if the traffic poses an imminent threat or is definitively identified as originating illegal robocall campaigns. Repeated violations will result in permanent service termination.

Section 2: Commitment to Traceback Cooperation (47 CFR § 64.6305(d)(iii))

RadWeb is fully committed to responding to and cooperating with all legal and regulatory requests, including those issued by the FCC, law enforcement, and the Industry Traceback Group (ITG).

2.1. Traceback Contact and Availability

- **Designated Point of Contact:** The Company maintains an internal compliance team responsible for receiving and processing traceback requests. The designated contact information is kept current within the Robocall Mitigation Database.
- **24/7 Availability:** The Company's technical and compliance teams maintain processes to ensure that critical traceback requests are received, acknowledged, and addressed promptly, regardless of time of day or day of the week, in compliance with ITG protocols.

2.2. Traceback Process and Cooperation

- **Speed of Response:** The Company commits to providing complete and accurate information relevant to a traceback request—including call detail records, customer identity, and call origination details—in the shortest time practicable.
- **Information Integrity:** We maintain accurate and complete records of all call traffic and customer provisioning data necessary to perform effective traceback.
- **Internal Investigation:** In response to a request, the Company will not only provide records but will also initiate an internal investigation to identify the source of the traffic and take immediate mitigation steps, including traffic blocking and service suspension as necessary, as outlined in Section 1.3.

By filing this description, RadWeb affirms its commitment to actively mitigate illegal robocall traffic originating from its network and to fully cooperate with all authorized traceback efforts.

Date of Filing: 2025-12-07