

ROBOCALL MITIGATION PLAN Rural Telecom Experts Inc. (RTE)

Overview

Rural Telecom Experts Inc. ("RTE") is a facilities-based Competitive Local Exchange Carrier (CLEC) operating within the United States. Pursuant to 47 C.F.R. § 64.6305, RTE submits this Robocall Mitigation Plan ("RMP") describing its practices and procedures to prevent, mitigate, and eliminate illegal robocall traffic originating from or traversing its network.

RTE is classified as a **small provider** and is eligible for the FCC's two-year extension for full STIR/SHAKEN implementation. RTE is working diligently to implement STIR/SHAKEN call authentication across its IP-based network. For non-IP network segments where STIR/SHAKEN is not yet deployed, RTE has implemented alternative robocall mitigation measures compliant with 47 C.F.R. § 64.6305.

RTE is committed to complying with the FCC's Robocalling Fourth Report and Order (FCC 20-187), the TRACED Act, and all applicable federal and state laws regarding illegal robocalls.

Traceback Compliance (24-Hour Response)

RTE commits to the following traceback obligations:

- RTE will respond to all traceback requests from the **FCC, law enforcement, and the Industry Traceback Group (ITG)** within **24 hours of receipt**.
 - RTE will designate a primary and secondary traceback contact point accessible 24/7/365.
 - RTE will cooperate fully with ITG-led traceback investigations and implement mitigation measures identified during such investigations.
-

ITG Compliance

RTE is an active participant in industry robocall mitigation efforts and will:

- Cooperate fully with the **Industry Traceback Group (ITG)** as the designated consortium for robocall traceback.
- Respond to ITG traceback requests within **24 hours**.
- Implement ITG-identified mitigation measures, including blocking or suspending traffic from verified illegal robocall sources.
- Participate in regular industry calls and information-sharing initiatives regarding robocall trends and mitigation strategies.

Robocall Mitigation Commitments

1. **Contractual Controls** – All RTE customers must sign an agreement affirming compliance with FCC, FTC, TCPA, and all applicable laws prohibiting illegal robocalls. Customers agree to immediate blocking or service termination for violations.
2. **Know Your Customer (KYC)** – RTE collects and verifies for all wholesale, enterprise, and call center customers: physical business address, primary contact, incorporation documents, Federal Tax ID (if applicable), USAC ID (FCC 499), banking information, and business nature.
3. **Continuous Traffic Monitoring** – RTE continuously monitors calling patterns to identify fraudulent traffic, including robocalls, traffic pumping, and toll fraud. RTE will block or terminate services for intentional violations.
4. **Robocall Mitigation Database Compliance** – After September 28, 2021, RTE only accepts traffic for termination from carriers and operators listed in the FCC's Robocall Mitigation Database.
5. **Blocking & Rate-Limiting** – RTE will block or rate-limit traffic from any upstream provider that fails to respond to traceback requests within 24 hours or that is identified as a source of illegal robocalls.
6. **STIR/SHAKEN Implementation (In Progress)** – As a small provider with an extension, RTE is actively implementing STIR/SHAKEN across its IP network. For non-IP segments, RTE applies alternative mitigation measures as permitted under FCC rules.
7. **Traceback Response** – RTE responds to all traceback requests from FCC, law enforcement, and ITG within **24 hours**.
8. **Continuous Improvement** – RTE will update this plan as industry best practices evolve.

Know Your Customer (KYC) & Monitoring Procedures

RTE implements the following specific measures:

- New account testing and turn-up monitoring for suspect traffic
 - Acceptable Use Policy (AUP) with blocking/suspension/termination rights
 - Account-specific profile numbers with traffic tagging and monitoring
 - Directory of IP addresses from SIP headers for tracking suspect traffic
 - Periodic calls with downstream carriers on traffic trends
 - Direct communication links with law enforcement
 - Industry seminars and fraud prevention workshops
 - Daily traffic reports with anomaly detection and carrier follow-up
 - Google search, social media review, incorporation verification, and FCC 499 cross-checking for all customers
-