

Robocall Mitigation Plan (RMP)

1. Executive Summary & Commitment

Provider Name: [Your Company Name]

FCC Registration Number (FRN): [Your FRN]

Date of Implementation: [Current Date]

[Company Name] is committed to protecting the integrity of the public switched telephone network (PSTN). This plan outlines the reasonable steps we take to prevent the origination, transit, and termination of illegal robocalls on our network, in compliance with the **TRACED Act** and **47 CFR § 64.6305**.

2. STIR/SHAKEN Implementation Status

Specify your current authentication status:

- **Full Implementation:** All IP calls are signed with STIR/SHAKEN.
- **Partial Implementation:** Some calls are signed; others use traditional TDM or are otherwise exempt.
- **Exemption:** If you do not have the facilities to implement STIR/SHAKEN, you must explain why and detail the alternative mitigation steps below.

Note for 2026: Providers using third-party signers must now maintain their own **SPC Token** and make all attestation level decisions themselves.

3. "Know Your Customer" (KYC) Procedures

The FCC requires a description of how you vet your customers to ensure they are not bad actors.

- **Identity Verification:** We collect and verify physical addresses, tax IDs, and authorized contact persons for all business entities.
- **Usage Analysis:** We evaluate the customer's business model (e.g., is it a call center?) to ensure the requested volume matches their legitimate business needs.
- **Service Agreements:** Our contracts include "Acceptable Use Policies" that explicitly prohibit illegal robocalling and spoofing, granting us the right to terminate service immediately for violations.

4. Call Analytics & Monitoring

Describe the technical tools you use to spot "robocall-like" behavior:

- **Traffic Pattern Analysis:** Real-time monitoring for high-volume bursts, low call completion rates (ACR), and short-duration calls.

- **Caller ID Validation:** Cross-referencing "From" numbers against known Do-Not-Originate (DNO) lists or invalid/unallocated number ranges.
- **Third-Party Tools:** (Optional) List any analytics vendors you use (e.g., TNS, Hiya, or Neustar).

5. Traceback Response Procedures

Providers must respond to "Traceback" requests from the **Industry Traceback Group (ITG)** or law enforcement.

- **24-Hour Commitment:** We commit to responding to all traceback requests within **24 hours** of receipt.
- **Dedicated POC:** Our Robocall Mitigation Point of Contact is:
 - **Name:** [Name]
 - **Email:** [Email]
 - **Phone:** [Phone Number]

6. Enforcement & Mitigation Actions

If illegal robocalling is detected, we take the following escalating steps:

1. **Immediate Investigation:** Contacting the subscriber to verify the traffic's legitimacy.
2. **Call Blocking:** Blocking specific traffic streams that are confirmed to be illegal or fraudulent.
3. **Service Termination:** Disconnecting customers who repeatedly violate robocall policies.

7. Annual Recertification & Compliance

- **Annual Filing:** We will recertify this plan in the **FCC Robocall Mitigation Database (RMD)** by **March 1st** of every year.
- **Updates:** Any change in company information or mitigation tactics will be updated in the RMD and CORES within **10 business days**.

Important Compliance Warning for 2026

- **Forfeitures:** The FCC now imposes a **\$10,000 base fine** for any false or inaccurate information in your RMD filing.
- **Daily Penalties:** Failure to update your information within 10 days of a change carries a **\$1,000 daily penalty** until cured.
- **MFA:** Ensure your RMD login uses Multi-Factor Authentication, as required by the latest security standards.