



Robocall Mitigation Plan (RMP)

Company: Callsy Network LLC

RMD Number: RMD0012433

1. STIR/SHAKEN Implementation

Callsy Network LLC has fully implemented the STIR/SHAKEN authentication framework across its network.

- All calls traversing our network must be signed with a minimum of a "C" attestation before routing to downstream carriers.
- Any unsigned calls are signed with a "C" attestation by Callsy Network LLC.
- Calls failing authentication are subject to filtering and blocking measures described in Section 4.

2. Traceback Requests ll traceback requests will be responded

to within **24 hours**.

- Internal tickets will be opened for any customer or upstream carrier identified in a traceback.
- Customers/upstream carriers must respond within 24 hours or face immediate account suspension.
- If **3 or more traceback requests** of different campaign types or dates lead back to the same customer/upstream carrier within 30 days, their account will be suspended for **90 days**.

Traceback Request Single Point of Contact:

- **Name:** GAURAV RAGHAV
- **Title:** DIRECTOR
- **Email Address:** gaurav@callsynetworkllc.com

3. Customer Vetting Practices

Callsy Network LLC employs rigorous Know Your Customer (KYC) procedures to minimize illegal robocall traffic. We collect and verify:

- Physical customer location, billing address, state/province, country, year of incorporation
- Contact person(s), federal tax ID, 499 ID, and RMD number
- Nature of business and traffic profile □ Participation in traceback processes
- History of enforcement actions, adverse judgments, or classification as “NonCooperative” or “Bad Actor” providers

Additionally, all customers/upstream carriers must provide trade and credit references.

4. Network Monitoring, Call Filtering, and Blocking

Callsy Network LLC uses advanced third-party platforms and analytic tools to detect and mitigate unlawful traffic.

- **Call Filtering:** Blocks invalid originating numbers, neighbourhood dialling, and numbers on the Somos® DNO list.
- **STIR/SHAKEN Enforcement:** Blocks all unsigned calls.
- **Block Lists:** Maintains internal and global block lists of numbers and IPs identified in ITG tracebacks or FCC enforcement actions.
- **Fraud Detection:** Utilizes real-time services (e.g., FraudCentral.io Roboguard) to identify and block known “Bad Actors.”
- **Monitoring:** Examines call detail records (CDRs) to detect suspicious patterns.

Actions taken include blocking numbers, notifying upstream carriers, and suspending accounts pending investigation.



5. Mandatory Blocking Following Commission Notification

Callsy Network LLC will promptly investigate and block any illegal traffic upon receiving a **Notice of Suspected Illegal Traffic** from the FCC's Enforcement Bureau.

6. Accepting Traffic Only from RMD-Listed Providers

In accordance with **47 C.F.R. § 64.6305(e) (1)**, Callsy Network LLC only accepts traffic from providers listed in the FCC's Robocall Mitigation Database.

7. Contractual Provisions and Acceptable Use Policy (AUP)

All customers must execute a **Master Service Agreement (MSA)** that requires compliance with all applicable telecommunications laws and regulations.

- Use of Callsy Network LLC's services for unlawful, fraudulent, abusive, or deceptive activity — including illegal robocalls, caller ID spoofing, or other non-compliant traffic — is strictly prohibited.
- Pursuant to the MSA and AUP, Callsy Network LLC may suspend or terminate services without prior notice to address violations, suspected fraud, regulatory obligations, or to protect network integrity.

8. Certification

Callsy Network LLC affirms that:

- Any prior certification filed in the RMD has not been removed or revoked by Commission action.
- Callsy Network LLC is not prohibited from filing or maintaining certification in the RMD.
- Updates to this RMP will be filed within **10 business days** of any material change.

