



Callvibe Network – Robocall Mitigation Plan

Overview

Callvibe Network is committed to preventing and mitigating illegal robocall traffic across its voice network. Our Robocall Mitigation Plan includes technical, contractual, and operational measures designed to protect end-users, comply with FCC guidelines, and support the traceback process.

1. Know Your Customer (KYC)

Callvibe Network verifies the identity of every commercial customer prior to onboarding. As part of our due diligence process, we collect:

- Legal business name
- Physical business address
- Federal Tax ID (TIN/W9)
- Country or state of incorporation
- FUSC 499 Filer ID (if applicable)
- FCC Registration Number (FRN)
- Robocall Mitigation Database (RMD) ID
- Traffic profile and routing intent
- LinkedIn profile and company website (if available)
- Identification of responsible contact person(s)

We do not onboard customers using generic email domains such as @gmail.com, @yahoo.com, or @outlook.com. All companies are screened by our compliance and legal team to determine a **trustability score** before access to the network is granted.

2. Traffic Monitoring and Analysis

Callvibe actively monitors its network for patterns that may indicate robocall activity. These include:

- High call volumes with short call durations
- Sequential dialing behavior
- Traffic to numbers on the FTC's National Do Not Call (DNC) Registry
- Sudden spikes in call attempts or anomalies in Answer Seizure Ratio (ASR)

We use automated alerts and manual audits to trigger internal investigations into any suspicious behavior.

3. Traceback Cooperation

All new and renegotiated customer contracts include a **mandatory traceback cooperation clause**. Callvibe promptly responds to traceback requests from:

- The FCC
- Law enforcement agencies
- The USTelecom Industry Traceback Group (ITG)
- Other authorized regulatory bodies

We identify either our direct customer or the upstream provider from which the suspicious traffic originated and share all relevant call detail records (CDRs), subject to applicable law and privacy protections.

4. Call Restrictions and Controls

If illegal robocall activity is suspected or confirmed, Callvibe may immediately impose the following mitigation measures:

- Call throttling and ASR limitations
- Blocking specific ANIs or destinations
- Limiting the number of concurrent calls
- Revoking caller ID privileges or requiring pre-approved ANI lists
- Suspending or terminating the account entirely

These actions may occur **without prior notice** when required to protect network integrity and regulatory compliance.

5. Contractual Enforcement

If a customer fails to cooperate in a traceback or is found in violation of our Acceptable Use Policy, Callvibe may take one or more of the following actions:

- Issue a formal notice of breach
- Suspend services pending investigation
- Terminate the agreement for cause
- Report the offending entity to appropriate authorities and industry partners

Continued violation after warnings will result in permanent disconnection.

6. Inbound Shielding and Caller ID Validation

Callvibe has implemented **Inbound Shield policies** using platforms such as TransNexus and other industry-standard tools. We query real-time databases to:

- Identify spoofed caller IDs
 - Flag high-risk or blacklisted numbers
 - Block calls originating from invalid or unassigned numbers
-

7. Required Caller ID and ANI Format

All calls originating through Callvibe must comply with the following ANI requirements:

1. ANIs must be valid, conforming U.S. numbers using the +1NPANXXYYYY format
 2. ANIs must match active blocks in the LERG database
 3. Spoofed ANIs or those producing unreturnable calls are strictly prohibited
 4. Government or sensitive agency impersonation (e.g., Social Security, IRS) is not tolerated and may be reported to authorities
 5. Calls to numbers on the DNC list may trigger regulatory action
-

8. Compliance Enforcement

Upon onboarding, Callvibe issues an official compliance notice to all customers stating:

- Robocalls, spam, scam, or missed-call fraud traffic is prohibited
 - Caller ID spoofing is not allowed
 - Violation of these rules may result in account suspension or formal reporting to the FCC, ITG, and other authorities
-

Contact & Enforcement Location

Callvibe Network

30 N Gould St Ste R Sheridan, WY 82801

www.callvibenetwork.com