



SENDBLUE ROBOCALL MITIGATION PROGRAM

1. Commitment to Mitigating Illegal Robocall Traffic

As a voice service provider, Sendblue is committed to preventing the origination of illegal robocall traffic on our network. Our robocall mitigation program includes the following components:

1.1 STIR/SHAKEN Framework Implementation:

- We have fully implemented the STIR/SHAKEN authentication framework across our entire network, ensuring compliance with § 64.6301(a)(1) and (2)
- We authenticate and verify caller identification information for all SIP calls transiting our network and for calls we originate

1.2 Strict User Authentication Policies:

- All calls are initiated through our secure software portal, accessible only to authenticated users through various methods of sign in
- Users must pass our authentication and verify their caller IDs before accessing calling capabilities.
- Only verified caller IDs are permitted to originate calls, ensuring accountability and traceability.

1.3 Proactive Measures to Avoid Illegal Traffic:

- Every customer is required to pass authentication before making a phone call from one of their verified caller IDs
- No user is permitted to make a phone call through our platform with any caller ID outside of the ones we have verified on their behalf.
- We perform continuous monitoring of call patterns to detect potential abuses.

1.4 Customer Verification and Monitoring:

- We personally know and work with all of our customers to validate customer identities and prevent misuse.
- Ongoing monitoring of user accounts and activity to ensure compliance with legal and ethical standards.

1.5 Cooperation with Authorities:

- We commit to respond within 24 hours to traceback requests from the FCC, law enforcement, and the Industry Traceback Group.
 - Full cooperation in identifying and stopping illegal robocallers using our network.
-

2. Procedures to Address Compliance History

2.1 Regulatory Investigations or Findings:

- At no time in the past two years has Sendblue been the subject of any formal action or investigation by the FCC, law enforcement, or other regulatory entities related to transmitting, encouraging, or facilitating illegal robocalls or spoofing.

2.2 Commitment to Transparency:

- Should any such investigations arise, we will promptly provide all required details, including involved parties, findings, and outcomes, to the appropriate authorities.
-

3. Traceback and Response Process

We prioritize swift and effective responses to traceback requests to assist in the investigation and mitigation of illegal robocall activities. Upon receiving a traceback request:

- A dedicated team initiates an investigation immediately.
 - A comprehensive response, including relevant findings and data, is provided within 24 hours to the requesting authority.
 - Corrective measures are implemented promptly to address any vulnerabilities identified.
-

4. Ongoing Program Enhancements

Our robocall mitigation program undergoes regular reviews to ensure effectiveness and compliance with emerging threats and regulatory updates. Updates to our program and certification details are submitted within 10 business days of any changes, in accordance with § 64.6305(d)(5).

For further information or updates to our Robocall Mitigation Program, please contact Robert Haber at rob@sendblue.com

