

Robocall Mitigation Program

Company Name: Strato VoIP

Service Type: VoIP / SIP Trunking Provider

Jurisdiction: United States (International Voice Traffic as Applicable)

1. Purpose and Scope

Strato VoIP is committed to preventing illegal robocalls, spoofing, and unlawful call origination across its network. This Robocall Mitigation Program outlines the policies, technical controls, monitoring procedures, and enforcement mechanisms implemented to ensure compliance with applicable U.S. regulations, including FCC requirements related to STIR/SHAKEN and robocall mitigation obligations.

This program applies to all inbound and outbound voice traffic transiting Strato VoIP's network.

2. STIR/SHAKEN Status

Strato VoIP implements STIR/SHAKEN authentication where technically feasible and applicable to its network architecture. For traffic that cannot be authenticated using STIR/SHAKEN (including certain international or legacy traffic), Strato VoIP applies the robocall mitigation measures described in this document.

3. Customer Due Diligence (KYC & Onboarding)

Strato VoIP performs due diligence prior to activating any customer, including but not limited to:

- Verification of customer identity and business registration
- Collection of legal business name, address, and authorized signatory
- Intended use of VoIP services and traffic profile disclosure
- Prohibition of illegal robocalling, spoofing, or fraudulent activity in customer agreements

Service is not activated until all required documentation is reviewed and approved.

4. Traffic Monitoring and Analytics

Strato VoIP actively monitors call traffic to identify potentially illegal or suspicious behavior. Monitoring includes:

- High call volume or burst detection
- Abnormal ASR (Answer-Seizure Ratio) and ACD (Average Call Duration) patterns
- Short-duration calls, call flooding, or repeated failed attempts
- Destination-based anomaly detection

Traffic is reviewed both automatically and manually by operations staff.

5. Prohibited Traffic

Strato VoIP strictly prohibits:

- Illegal robocalls
- Spoofed or misleading caller ID
- Auto-dialed calls without proper consent
- Scam, fraud, phishing, or impersonation traffic

Any traffic that violates U.S. federal or state laws, or upstream carrier policies, is not permitted.

6. Enforcement Actions

If suspicious or illegal activity is detected, Strato VoIP may take immediate action, including:

- Traffic throttling or blocking
- Temporary suspension of services
- Permanent termination of customer accounts
- Notification to upstream carriers or regulatory authorities, where required

Actions are taken without prior notice when necessary to protect network integrity.

7. Traceback Cooperation

Strato VoIP fully cooperates with:

- Industry Traceback Group (ITG) requests
- Law enforcement inquiries
- FCC or upstream carrier investigations

Call detail records (CDRs) and relevant data are retained and made available in accordance with legal requirements.

8. Network Controls and Safeguards

Technical safeguards implemented by Strato VoIP include:

- SIP authentication and IP whitelisting
- Call rate limiting and CPS thresholds
- Geo-blocking of high-risk destinations
- SBC (Session Border Controller) protections
- Firewall and access control enforcement

These controls reduce exposure to robocall abuse and network misuse.

9. Ongoing Review and Updates

Strato VoIP reviews and updates its Robocall Mitigation Program periodically to ensure continued compliance with regulatory changes, FCC guidance, and industry best practices.

10. Certification

Strato VoIP certifies that it has implemented the robocall mitigation practices described above and will take reasonable and effective steps to prevent the origination of illegal robocalls on its network.