



Robocall Mitigation Program Description

Submitted to the Federal Communications Commission – Robocall Mitigation Database

I. Provider Information

Legal Name:	VoxSun Inc.
d/b/a:	VoxSun
Principal Business Address:	2810 North Church Street, Wilmington, DE 19802
Provider Type:	Voice Service Provider (B2B Cloud VoIP Carrier)
FCC Registration:	Registered with the Federal Communications Commission (FCC)
CRTC Registration:	Registered with the Canadian Radio-television and Telecommunications Commission
Service Territory:	United States (FCC-regulated traffic) and Canada
Customer Base:	Business customers only (enterprise lines); no residential end-users

II. STIR/SHAKEN Implementation Status

VoxSun Telecom has **fully implemented STIR/SHAKEN caller ID authentication** on the IP portions of its network in accordance with the FCC's rules and the ATIS/SIP Forum SHAKEN standards. VoxSun is an authorized Certification Authority (CA) participant and holds a valid Service Provider Code (SPC) Token issued by the STI-PA (Secure Telephone Identity Policy Administrator).

VoxSun applies STIR/SHAKEN attestation levels as follows:

- **Full Attestation (Level A):** Applied when VoxSun has authenticated the calling party's identity and confirmed that the customer is authorized to use the asserted telephone number (TN), consistent with ATIS-1000089.
- **Partial Attestation (Level B):** Applied when VoxSun has authenticated the originating gateway but cannot fully verify the end-user's right to assert the specific calling number.
- **Gateway Attestation (Level C):** Applied to calls received from non-verified upstream sources at an international or non-IP gateway.

III. Mechanism for Determining User's Right to Assert a Number

VoxSun serves exclusively business customers (enterprise lines) and verifies each customer's right to assert a calling party number (CLI) prior to permitting its use for outbound calls. Verification is accomplished through one of the following methods:

A. Direct Number Assignment

When a telephone number is provisioned directly by VoxSun and assigned to a customer account, it is automatically validated within VoxSun's internal numbering management system. Only numbers linked to a given account may be presented as the outbound caller ID for that account.

B. Customer-Provided Numbers (Bring Your Own Number – BYON)

For numbers not assigned by VoxSun, the customer must provide proof of ownership or authorization before the number is enabled for outbound use. Acceptable evidence includes:

- A recent invoice or Letter of Authorization (LOA) from the number's current carrier of record;
- A real-time verification call or one-time passcode (OTP) delivered to the number in question; or
- WHOIS or Local Number Portability (LNP) database validation, where available.

Upon successful verification, the number is flagged as 'authorized' in the customer's provisioning record and made available for outbound use.

C. Internal Telephone Number Database

VoxSun maintains a centralized internal telephone number database that records:

- Customer account identifiers;
- Authorized TNs (Telephone Numbers) associated with each account;
- Verification method and timestamp for each authorized TN;
- Number status (active, revoked, or pending).

This database is populated automatically for VoxSun-assigned numbers through provisioning workflows and manually or semi-automatically for customer-provided numbers following validation. It is kept synchronized with the STIR/SHAKEN signing service to ensure that only numbers with confirmed authorization receive Full Attestation (Level A) signatures.

D. Alignment with ATIS-1000089

VoxSun's number-assertion mechanism aligns with the Full Attestation Alternatives defined in ATIS-1000089, specifically the model in which the service provider maintains a verified association between the subscriber and the calling number prior to signing.

IV. Affirmative Measures to Prevent Customers from Originating Illegal Robocalls

Because VoxSun provides service exclusively to businesses, its customer onboarding and acceptable-use framework constitutes a primary layer of robocall prevention. VoxSun takes the following affirmative steps:

Know Your Customer (KYC): Prior to activating service, VoxSun verifies business identity through business registration documents, government-issued identification of authorized officers, and proof of business address. Residential or anonymous customers are not accepted.

Acceptable Use Policy (AUP): All customers execute a service agreement that explicitly prohibits the origination of illegal robocalls, unsolicited commercial calls without prior express consent, caller ID spoofing, and any other conduct prohibited by the Telephone Consumer Protection Act (TCPA), Truth in Caller ID Act, and applicable FCC rules.

Call Volume Monitoring: VoxSun monitors call detail records (CDRs) for anomalous patterns including abnormally high call volumes, sequential dialing to consecutive numbers, unusually short call durations, high abandonment rates, and repeated dialing to numbers on the National Do Not Call Registry.

Automated Alerting: Threshold-based alerts are triggered for accounts exhibiting suspicious traffic profiles, initiating a compliance review. Accounts confirmed to be originating illegal traffic are suspended immediately.

Contractual Enforcement: VoxSun's service agreements authorize immediate suspension or termination of accounts found to be in violation of the AUP, with no obligation of advance notice where illegal robocalling is confirmed.

V. Know-Your-Upstream-Provider Program

When VoxSun accepts call traffic from upstream voice service providers or intermediate providers, it applies the following practices:

- VoxSun accepts interconnect traffic only from providers that are listed in the FCC Robocall Mitigation Database (RMD) or that have otherwise demonstrated compliance with applicable FCC rules.
- Upstream provider credentials, including RMD listing status, are verified prior to establishing interconnection and reviewed periodically.
- VoxSun monitors inbound traffic from upstream providers for suspicious patterns and reserves the right to block or suspend interconnection where evidence of illegal robocall origination is detected.
- Interconnection agreements include provisions requiring upstream providers to cooperate with traceback investigations and comply with FCC robocall mitigation rules.

VI. Call Analytics Systems

VoxSun employs the following call analytics and monitoring measures to identify and block illegal robocall traffic:

Internal CDR Analytics: VoxSun's network operations team analyzes call detail records on an ongoing basis, with particular attention to: (1) traffic volume spikes or bursts in narrow time windows; (2) high-volume outbound campaigns to sequential or closely-grouped number ranges; (3) calls to NPA-NXX blocks not assigned by NANPA; (4) calls to numbers on the National Do Not Call Registry; and (5) anomalously low call-completion ratios.

Caller ID Integrity Checks: VoxSun's STIR/SHAKEN infrastructure validates each outbound call against the authorized TN database before assigning an attestation level, providing a built-in control against caller ID spoofing.

Third-Party Analytics: VoxSun leverages third-party call analytics tools to supplement internal monitoring capabilities and to cross-reference known illegal robocall campaigns identified by the Industry Traceback Group (ITG) and other industry bodies.

VII. Traceback Cooperation

VoxSun is committed to full and timely cooperation with traceback investigations conducted by the FCC, law enforcement agencies, and the Industry Traceback Group (ITG). Specifically:

- VoxSun designates a single point of contact (identified below) responsible for receiving and responding to all traceback requests.
- VoxSun commits to responding to traceback requests within the timeframes established by the ITG and the FCC.
- VoxSun retains call detail records sufficient to support traceback investigations for a period consistent with FCC retention requirements.
- Where a customer is identified as the source of illegal robocall traffic through a traceback investigation, VoxSun will take immediate corrective action, including suspension or termination of the account.
- Interconnection and service agreements include provisions requiring downstream customers and upstream providers to cooperate with traceback requests.

VIII. Enforcement History

VoxSun Telecom has not been the subject of any FCC enforcement action related to robocalling, illegal caller ID spoofing, or STIR/SHAKEN non-compliance. No certification filed by VoxSun in the Robocall Mitigation Database has been removed by Commission action, and VoxSun has not been prohibited from filing in the Robocall Mitigation Database.

IX. Robocall Mitigation Point of Contact

Company:	VoxSun Inc.
Role:	Designated Robocall Mitigation Compliance Contact
Mailing Address:	2810 North Church Street, Wilmington, DE 19802
Email:	[compliance contact email]
Phone:	[compliance contact telephone number]

X. Certification

The undersigned, acting as an authorized representative of VoxSun Inc., hereby certifies under penalty of perjury that the information contained in this Robocall Mitigation Program Description is true, complete, and accurate to the best of the undersigned's knowledge, information, and belief. VoxSun Telecom certifies that all calls it originates on its network are subject to the robocall mitigation program described herein, and that this certification has not been removed by Commission action and VoxSun has not been prohibited from filing in the Robocall Mitigation Database.

Signature: _____

Name: _____

Title: _____

Date: _____

This document constitutes VoxSun Telecom's Robocall Mitigation Program Description as required by 47 CFR § 64.6305 and the FCC's Robocall Mitigation Database filing requirements. This document should be submitted as a PDF attachment to VoxSun's Robocall Mitigation Database certification filing via the FCC's Electronic Comment Filing System (ECFS) portal at <https://fccprod.servicenowservices.com/rmd>.