

Zonitel Solutions LLC
ROBOCALL MITIGATION PLAN
UPDATED - FEBRUARY 2026

1. PURPOSE AND SCOPE

Zonitel Solutions LLC (the “Provider”) is a voice service provider that originates voice traffic to the public switched telephone network (PSTN) and maintains a robocall mitigation program consistent with 47 CFR § 64.6305, including STIR/SHAKEN caller ID authentication implemented pursuant to 47 CFR § 64.6301(a).

2. PROVIDER ROLE / CALL FLOW

Zonitel Solutions LLC provides cloud voice services to business customers, including hosted PBX/VoIP seat service, SIP trunking, DID provisioning/management, inbound/outbound calling, and related call routing features. Customers are primarily retail/SMB and enterprise end users; in limited cases we support reseller/agent-led deployments for end-user business accounts.

Our traffic is both originated and carried/processed on our network. Calls can originate from end-user endpoints (phones/softphones/customer PBX) registered to or interconnected with our platform and are routed to the PSTN via our upstream carrier partner(s). We also carry and process inbound calls to numbering resources we manage and deliver those calls to customer endpoints.

3. STIR/SHAKEN STATUS

Zonitel Solutions LLC certifies that it has implemented STIR/SHAKEN caller ID authentication across its IP network for the calls it originates, consistent with 47 CFR § 64.6301(a). The Provider’s network is IP-based for SIP calling, and the Provider authenticates caller identification information for SIP calls it originates and, to the extent technically feasible, transmits calls with authenticated caller identification information to the next voice service provider or intermediate provider in the call path.

The Provider signs outbound calls it originates using its own STI certificate issued by an approved STI Certificate Authority (STI-CA). Identity headers are passed downstream unchanged. For inbound SIP calls received for termination/delivery to end users where the caller identification information has been authenticated, the Provider verifies caller identification information where technically feasible.

The Provider assigns attestation levels based on its verification of the calling party and confirmation of the calling party’s authority to originate calls using the associated telephone number(s), consistent with applicable FCC rules, orders, and guidance.

4. ROBOCALL MITIGATION MEASURES

a. KNOW YOUR CUSTOMER PROCEDURES

The Provider takes affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence to ensure its services are not used to originate illegal traffic.

At onboarding, we collect and verify business identity and authority details, including (as

applicable): legal business name, DBA, EIN and/or formation documents, service address, authorized representative, email/phone, and payment method. For any numbers provisioned or ported, we confirm the customer's control/authorization for the telephone numbers (e.g., porting/LOA documentation and/or other proof of authority, as applicable).

We validate customers using a risk-based review as appropriate, including review of public business records where applicable (e.g., Secretary of State listings), consistency of contact details, and reasonableness of the requested services and use case. We gather the expected use case (industry, call purpose, target geography), anticipated volumes, and calling patterns (inbound/outbound mix, peak expectations) prior to enabling outbound services.

Enhanced review is triggered by high-risk verticals, unusually high projected volume, discrepancies in identity/authorization, repeated changes to caller ID, short-lived accounts, or any indicators of lead-generation/robocall behavior inconsistent with the stated use case.

Additionally, we maintain Terms of Service and an Acceptable Use Policy that prohibit illegal robocalls, spoofing/unauthorized caller ID, misuse of numbering resources, and other unlawful or abusive calling activity. Customer agreements reserve our right to investigate, rate-limit, block, suspend, or terminate service for suspected or confirmed violations and to require supporting documentation when warranted.

b. TRAFFIC MONITORING, ANALYTICS, AND ENFORCEMENT

We continuously monitor traffic patterns and call performance metrics with our internal systems to detect suspicious behavior, including bursting/spike patterns, abnormal ASR/ACD, short-duration call bursts, high invalid/unallocated destinations, and inconsistent/invalid caller ID patterns. Caller ID is limited to numbers provisioned/porting to the customer account; unauthorized CLI is blocked. In addition to our in-house solutions, we utilize third-party analytics and feedback signals provided by Bandwidth, Inc. (Bandwidth.com) (our upstream carrier partner) for robocall/spam labeling and blocking outcomes, including robocall/spam indicators and blocking feedback, to identify potentially illegal or unwanted traffic. When suspicious or illegal traffic is detected, our escalation typically follows:

- i. investigate and contact customer
- ii. warn and request remediation/supporting documentation
- iii. rate-limit or temporarily block affected traffic/caller IDs
- iv. suspend service if unresolved
- v. terminate service for repeat or confirmed abuse, and we cooperate with upstream carriers and applicable traceback requests when required.

c. KNOW YOUR UPSTREAM PROVIDERS

KYUP applies to the Company's upstream carrier relationships that enable PSTN interconnection and numbering resources. The Company's primary carrier is Bandwidth, Inc. (Bandwidth.com). The Company validates upstream provider identity and contractual authority, maintains current

escalation/traceback points of contact, and confirms the upstream provider supports robocall mitigation and traceback cooperation (including access to call detail records and timely response procedures). The Company reviews upstream performance on a periodic basis and upon material changes or indicators of suspected illegal traffic (e.g., complaints, abnormal traffic patterns, analytics flags, or traceback notices) and escalates issues for investigation and remediation.

In limited reseller/agent-led deployments, the Company applies the same KYC onboarding controls used for direct end-user customers, with enhanced review (entity/principal verification, documented end-user use case, expected volumes, and contractual restrictions on unlawful robocalling). Where issues are identified, the Company will implement mitigation measures within its control (including blocking/suspension of offending traffic sources where applicable) and coordinate with the upstream provider to prevent continued transmission of illegal robocall traffic.

d. ROBOCALL MITIGATION / TRACEBACK CONTACT

Name: Abel Arias

Title/Department: Manager / Administration

Email: info@zonitel.com

Phone: 833-966-4835

Business Address: 403 W GRAND PARKWAY S SUITE F -304, Katy TX 77494

e. PRIOR TWO-YEAR ACTIONS / INVESTIGATIONS (RMD DISCLOSURE)

Zonitel Solutions LLC states that, during the prior two (2) years, neither Zonitel Solutions LLC nor any entity for which Zonitel Solutions LLC shares common ownership, management, directors, or control has been the subject of a formal FCC, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing related to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

5. TRACEBACK COOPERATION AND RESPONSE

The Provider remains committed to responding fully and within 24 hours (measured in business hours, as applicable) to call traceback requests from the Commission, law enforcement, and the traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers initiating calls.

6. ONGOING EFFORTS AND UPDATES

Zonitel Solutions LLC is committed to maintaining and improving its robocall mitigation practices, including:

- Updating its RMD filing and associated plan information within 10 business days when filing information changes.
- Regular review and updates to the mitigation program to address emerging threats and regulatory changes.

- Participation in industry forums and initiatives to develop best practices for combating illegal robocalls.
- Educating our consumers on how to avoid being a victim of illegal robocalls and providing a method for reporting robocall-related concerns.