

ROBOCALL MITIGATION PROGRAM DESCRIPTION

The ZEGs Corp,

DBA: ZEGIT Tech Solutions

Date: 3/27/2026

1. Introduction and Certification

The ZEGs Corp (DBA, ZEGIT Tech Solutions) is a Managed Service Provider (MSP) that resells VoIP services, including SIP trunks and hosted PBX systems, to business customers in the United States. We certify that all calls originated via our service are subject to this Robocall Mitigation Program, which includes reasonable steps to prevent the origination of illegal robocalls consistent with 47 CFR § 64.6305(a). We further certify that we have not been prohibited from filing in the Robocall Mitigation Database and that any prior certification has not been removed by Commission action.

We have no STIR/SHAKEN implementation on any portion of our operations because, as a non-facilities-based reseller, we do not control the underlying IP network or SIP signaling infrastructure (see exemption explanation filed with this submission).

2. STIR/SHAKEN Status

We have not implemented the STIR/SHAKEN authentication framework on any portion of our network. All call origination and SIP handling occurs on our upstream wholesale provider's network.

3. Reasonable Steps to Prevent Illegal Robocalls

A. Customer Vetting (Know-Your-Customer / KYC)

- i. We take affirmative, effective measures to vet all new and renewing customers to ensure they are legitimate and do not intend to originate illegal robocalls:
 - i. No account is activated solely via email or online form. Every customer must speak directly with a ZEGIT representative either in person or by phone at least once during the onboarding process.
- ii. We conduct a live discussion of the customer's intended use of the SIP trunk / hosted PBX service and document the legitimate business purpose (e.g., standard office telephony, customer service lines, etc.).

- iii. We require and review government-issued photo ID of the account holder, business formation documents, physical address verification, and contact information.
- iv. We review the customer's website (if any) and any other publicly available information to confirm legitimacy.
- v. High-risk indicators (e.g., requests for high-volume outbound calling, international termination patterns inconsistent with stated business, or unusual traffic requests) trigger additional scrutiny or denial of service.

B. Master Service Agreement (MSA) and Prohibited Uses

Every customer must sign our MSA, which explicitly:

- Prohibits the origination of illegal robocalls, spoofing, or any traffic that violates FCC rules (including 47 CFR § 64.1200 and the TRACED Act).
- Requires customers to use the service only for lawful purposes.
- Authorizes ZEGIT Tech Solutions (The ZEGs Corp) to immediately suspend or terminate service upon evidence of illegal robocall activity.
- Instructs customers that they must also comply with all applicable robocall mitigation obligations if they further resell the service.

A copy of the relevant MSA sections is maintained in our records.

C. Upstream Provider Vetting

We only accept traffic from a single vetted upstream wholesale VoIP provider (currently in the process of becoming an authorized reseller of VoIP.ms). We have confirmed that the upstream provider maintains its own robust robocall mitigation and STIR/SHAKEN program where applicable. We monitor the upstream provider's status in the Robocall Mitigation Database and will immediately cease using any upstream provider whose certification is removed or who fails to cooperate with traceback. Contact information for the upstream provider's abuse/traceback team is on file and updated regularly.

D. Call Monitoring and Analytics

We actively monitor call traffic patterns to detect and prevent illegal robocall activity using the following reasonable steps:

- Daily/weekly review of call detail records (CDR) provided by our upstream provider, focusing on anomalous patterns such as unusually high call volume in short time periods, very short average call duration (<10 seconds), high answer-seizure ratios inconsistent with stated business use, or sudden spikes in outbound traffic.
- Manual investigation of any flagged traffic by our operations team.

- If suspicious patterns are identified, we immediately contact the customer for explanation and, if necessary, block or terminate the affected numbers/lines.
- We maintain logs of all investigations.

(We currently rely on upstream-provided analytics dashboards and manual CDR review; we will evaluate third-party robocall analytics tools as our volume grows.)

E. Traceback Cooperation and Enforcement

We commit to responding fully and within 24 hours to all traceback requests from the FCC, law enforcement, and the Industry Traceback Consortium (ITC/ITG).

Designated point of contact: James Zeglin, President, 763-284-9904, jzeglin@zegittech.com.

Upon receipt of a traceback request, we will promptly pull relevant CDRs, customer information, and any investigation notes and provide them to the requesting entity.

If illegal activity is confirmed, we will immediately suspend the offending customer/line and cooperate fully in any investigation.

We will terminate service to any customer found to be originating illegal robocalls and will not re-activate until the issue is fully resolved to our satisfaction and the authorities'.

4. Ongoing Review

This Robocall Mitigation Program is reviewed and updated annually (or more frequently if FCC rules change). We will publish a current version on our website and notify all customers of any material updates.

5. Contact Information

The ZEGs Corp
DBA: ZEGIT Tech Solutions
14332 286 ½ Ave NW
Zimmerman, MN 55398

Compliance Contact: James Zeglin, President

Phone: 763-284-9904

Email: jzeglin@zegittech.com