

Robocall Mitigation Program Description

Cenos Networks

Date: March 5, 2026

Submitted Pursuant to 47 CFR § 64.6305(d)

1. Company Overview

Cenos Networks is a Mobile Virtual Network Operator (MVNO) that provides mobile wireless voice and data services to business customers in the United States. Cenoss Networks resells voice and data services provided over the network infrastructure of AT&T. Cenoss Networks does not own, operate, or control any telecommunications network infrastructure. All calls originated by Cenoss Networks customers are transmitted over AT&T's network.

2. STIR/SHAKEN Implementation Status and Exemption

Cenos Networks certifies that it has not implemented the STIR/SHAKEN authentication framework on any portion of its network, pursuant to Option 3 of the Voice Service Provider Certification.

As an MVNO, Cenoss Networks does not own or control the network infrastructure necessary to implement STIR/SHAKEN. Specifically, Cenoss Networks:

- Does not operate its own network switches, routing equipment, or IP infrastructure;
- Does not have the ability to obtain a Service Provider Code (SPC) token from the STIR/SHAKEN Policy Administrator for the purpose of signing calls on its own network;
- Transmits all customer voice traffic over AT&T's network, which is responsible for call origination and authentication at the network layer.

This exemption is claimed pursuant to 47 CFR § 64.6301(b), which recognizes that providers lacking control over the network infrastructure necessary to implement STIR/SHAKEN are not required to do so independently. AT&T, as the underlying network provider, maintains its own RMD filing and STIR/SHAKEN implementation. Cenoss Networks' inability to implement STIR/SHAKEN is a direct consequence of its status as a network infrastructure-less reseller, not a failure of compliance effort.

3. Robocall Mitigation Program

Although Cenoss Networks does not control the underlying network infrastructure, Cenoss Networks has implemented a robocall mitigation program consistent with 47 CFR § 64.6305(a). This program includes the specific steps described below to avoid originating illegal robocall traffic.

3.1 Know Your Customer (KYC) Procedures

Cenos Networks serves business customers exclusively. All prospective customers are subject to a manual review and approval process prior to activation of service. This process includes:

- Verification of business identity, including legal business name, principal place of business, and contact information;
- Review of the intended use case for voice services to assess whether the requested usage is consistent with legitimate business operations;
- Manual approval by Cenos Networks personnel before any account is activated for voice services;
- Retention of customer account records including business name, contact information, and service agreements.

Cenos Networks does not activate voice service for customers whose intended use raises concerns about potential illegal robocall activity, including but not limited to high-volume outbound calling operations that lack a clear legitimate business purpose.

Cenos Networks complies with its know-your-customer obligations pursuant to 47 CFR § 64.1200(n)(4).

3.2 Upstream Provider Relationship

Cenos Networks provides voice services exclusively through AT&T as its underlying network provider. AT&T is a major U.S. facilities-based carrier with its own STIR/SHAKEN implementation and RMD filing. Cenos Networks has a contractual relationship with AT&T governing the provision of wholesale voice services. All customer voice traffic is carried over AT&T's network infrastructure.

Cenos Networks does not have additional upstream voice providers for its MVNO voice services. Cenos Networks monitors its upstream provider relationship and would take commercially reasonable steps to address any concerns about the integrity of traffic flowing through that relationship.

3.3 Traffic Analytics and Monitoring

Cenos Networks does not independently operate traffic analytics or call monitoring systems, as all voice traffic is carried on and monitored by AT&T's network infrastructure. Cenos Networks relies on AT&T's network-level traffic analytics and fraud detection systems, which are part of AT&T's own robocall mitigation program.

Cenos Networks does not use any third-party analytics vendors for robocall traffic monitoring. Cenos Networks does not currently subscribe to independent third-party call analytics services.

At the account management level, Cenoss Networks monitors customer accounts for unusual usage patterns. Accounts exhibiting anomalous activity — such as sudden spikes in outbound call volume inconsistent with prior usage — are subject to manual review. Cenoss Networks may suspend or terminate accounts found to be generating traffic that appears to facilitate illegal robocalling activity.

3.4 Response to Illegal Traffic

If Cenoss Networks becomes aware that a customer is using its service to originate illegal robocall traffic, Cenoss Networks will take the following steps:

1. Immediately investigate the customer account and the nature of the traffic in question;
2. Suspend or terminate the customer account if the investigation confirms illegal robocall activity;
3. Notify AT&T of the suspected illegal traffic so that appropriate action can be taken at the network level;
4. Cooperate fully with any investigation by the FCC, law enforcement, or the industry traceback consortium.

4. Traceback Commitment

Cenoss Networks commits to respond fully and within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement agencies, and the industry traceback consortium (USTelecom's Industry Traceback Group), and to cooperate fully with such entities in investigating and stopping any illegal robocallers that use Cenoss Networks' service to originate calls.

The designated point of contact for robocall mitigation and traceback requests is identified in Cenoss Networks' Robocall Mitigation Database filing. Cenoss Networks will update this contact information within 10 business days of any change, consistent with 47 CFR § 64.6305(d)(5).

5. Prior Government Actions or Investigations

Cenoss Networks certifies that it has not, at any time in the prior two years, been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

No affiliated entities sharing common ownership, management, directors, or control with Cenoss Networks have been subject to such actions or investigations during this period.