

Robocall Mitigation Program

This Robocall Mitigation Program ("Program") is adopted to comply with the requirements of 47 CFR § 64.6305(d)(ii)-(iii) applicable to Thumb Electric Cooperative and its affiliates. This Program describes the specific reasonable steps implemented to prevent the origination and transmission of illegal robocalls and details the process used to mitigate such traffic on the provider's network.

1. STIR/SHAKEN Implementation Status

The provider has implemented the STIR/SHAKEN caller ID authentication framework in the IP portions of its network as required by applicable FCC rules. Where full end-to-end IP functionality exists, the provider authenticates outbound calls and verifies inbound calls using approved authentication certificates. Calls are attested at the appropriate level based on customer relationship and knowledge of the calling party.

2. Mitigation of Non-IP and Other Traffic

For any portions of the network not capable of full STIR/SHAKEN implementation, including TDM or other non-IP segments, the provider has established alternative robocall mitigation measures designed to reasonably reduce the risk of originating or transmitting illegal robocalls.

- Know-Your-Customer (KYC) procedures prior to provisioning voice service, including identity verification and validation of business purpose.
- Contractual provisions prohibiting customers from originating illegal robocalls and requiring compliance with federal and state telemarketing laws.
- Traffic monitoring analytics to detect unusual volume spikes, short duration calls, sequential dialing patterns, and other high-risk indicators.
- Prompt investigation and suspension of traffic associated with traceback requests or credible evidence of illegal robocall activity.
- Participation in industry traceback efforts and cooperation with law enforcement and regulatory authorities.
- Maintenance of internal escalation procedures for rapid response to suspected illegal robocall traffic.

3. Response to Traceback and Enforcement Notices

The provider responds promptly to traceback requests from the Industry Traceback Group or other authorized entities. Upon receipt of credible notification that a customer or upstream provider is transmitting illegal robocalls, the provider investigates the traffic, takes appropriate remedial action, and where necessary suspends or terminates service. All mitigation actions are documented and retained in accordance with internal compliance policies.

4. Ongoing Monitoring and Program Review

The provider conducts ongoing monitoring of outbound and inbound call traffic to detect potentially unlawful robocalls. Compliance personnel periodically review this Program to ensure continued effectiveness and alignment with evolving FCC guidance and industry best practices. Training is provided to relevant employees regarding robocall detection and mitigation obligations.

5. Certification

The provider certifies that it has implemented the mitigation practices described herein and that it will continue to take reasonable steps to prevent the origination and transmission of illegal robocalls, consistent with 47 CFR § 64.6305(d)(ii)-(iii). This Program is maintained as part of the provider's Robocall Mitigation Database filing and will be updated as required by law.

Authorized Representative: Kevin Mazure

Title: Director of Administrative Services

Date: 2/25/2026