

Robocall Mitigation Plan
FEDERATED RURAL ELECTRIC ASSN.

FRN: 0002-6527-41

Filing Date: February 11, 2026

The following documentation is to serve as the Robocall Mitigation Plan of FEDERATED RURAL ELECTRIC ASSN. (Company) and their ongoing compliance with the Traced Act.

COMPANY hereby certifies the following information:

The Company has not implemented the STIR/SHAKEN authentication framework on any portion of its network. The Company has committed to a RoboCall Mitigation Program consistent with 47 CFR § 64.6305 for all originating calls made from its network.

The Provider's contracted wholesaler, GigTel, has fully implemented the STIR-SHAKEN authentication framework across its entire network and all calls it originates are compliant with 47 CFR § 64.6301(a)(1) and (2). Further, the Provider and wholesaler have established the policies and procedures set forth in this Robocall Mitigation Plan which are intended to stop anyone from using the Provider's service to originate illegal robocalls.

The Company (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has not 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 the Company transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

COMPANY hereby certifies to the implementation of the following practices:

Traceback Requests

- a. Pursuant to 47 CFR § 64.6305(d)(4), the Company has designated a point of contact to receive notice of any incidents of illegal robocall traffic. This person's name, title, address, phone number, and email address are in the RoboCall Mitigation Database portal.
- b. This individual will be the main contact responding to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. Company will respond fully and within 24 hours to traceback requests from such entities and will cooperate in investigating and stopping any illegal robocallers that use its network to originate calls.

Subscriber Vetting Process

- c. Company will vet the identity of residential, retail, and wholesale subscribers through normal business practices and will obtain service address information.
- d. Company will complete an additional review of any outbound call centers or high-volume origination services within its network that may include a stricter application review process.

Telephone Validation Process

- e. A subscriber is permitted to use a telephone number as their caller identity, if a number is directly managed by Company and/or obtained by Company via an underlying partner. Company has established a process for ensuring subscribers are utilizing only telephone numbers assigned to them or have been authorized for use. For subscribers with a single line service, the Class 5 switch has been set up to only accept calls from the number assigned to that subscriber, for both services connected via TDM or IP, at the time-of-service origination. For subscribers with multi-line telephone systems (MLTS), for both services connected via TDM or IP, Company screens all originating calls and only allows the call to be connected if the originating telephone number matches one of the assigned numbers to that MLTS subscriber.

Network Monitoring Mitigation

- f. The Provider monitors the usage of its network through its wholesale provider GlgTel. When network usage patterns consistent with illegal robocalls are detected or the parties otherwise suspect illegal robocalling or spoofing is taking place on its network, it immediately seeks to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action. The actions taken may include, but are not limited to: initiating a traceback investigation; verifying that the originating customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name; terminating the party's ability to originate, terminate, or route calls on the Provider's network; and providing notice to law enforcement authorities.
- g. As part of its Plan to mitigate and prevent any originating robocalls on its network, the Provider through wholesaler GigTel, is committed to early identification and investigation of possible robocalling situations. In monitoring usage of its network, particular attention is given to: (1) higher than normal subscriber traffic volume including large bursts of traffic in small timeframes or inconsistent volumes of traffic (spikes in usage); (2) originating calls of short duration and low call completion percentages; (3) originating calls with sequential called to number dialing patterns; (4) calls made to do-not-call

registry or invalid numbers; and (5) calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator.

- h. Company has explored partnerships with third-party validation service providers that use analytics to identify the origination or termination of illegal robocalls. The Company, through its wholesale provider, uses TransNexus' call analytics system.

Know-Your-Upstream Provider

- i. The Company knows all the carriers from which it receives traffic and has confirmed that all carriers in which it exchanges traffic and from which it receives traffic are listed in the Robocall Mitigation Database. Basic identification information, such as physical business location, contact person(s), state of incorporation, and nature of business, are collected for all the Company's up-stream providers. Going forward, all interconnection agreements will include prohibited traffic and traceback language.