

Robocall Mitigation Plan
FEDERATED TELEPHONE COOPERATIVE

FRN: 0003-7415-76

Filing Date: February 17, 2026

The following documentation is to serve as the Robocall Mitigation Program of FEDERATED TELEPHONE COOPERATIVE (Company) and their ongoing compliance with the Traced Act.

47 CFR § 64.6304(d) – Non-IP networks allow for those portions of a voice service providers' network that rely on technology that cannot initiate, maintain, and terminate SIP calls are deemed subject to a continuing extension. A voice service provider subject to the foregoing extension shall comply with the requirements of 47 CFR § 64.6303 as to the portion of its network subject to the extension.

COMPANY hereby certifies the following information:

The Company has implemented the STIR/SHAKEN authentication framework on a portion of its network, and all calls it originates on that portion of its network are compliant with 47 CFR § 64.6301(a)(1) and (2).

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:

Implement STIR/SHAKEN call authentication

- a. Company is compliant with the IP portion of their network using a third-party service.

Traceback Request

- b. Pursuant to 47 CFR § 64.6305(d)(4)(v), 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.
- c. 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

- d. Company will vet the identity of retail and wholesale subscribers, in conjunction with (i) approving applications for service; (ii) provisioning network connectivity; (iii) entering into any contract agreements; or (iv) granting the right-to-use telephone number resources. In its vetting process, Company will confirm the identity of new or renewing business customers by collecting information such as the following:
 - a. physical business location
 - b. a contact person for the business
 - c. state or country of incorporation
 - d. federal tax ID
- e. 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

- f. 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

- g. **Analyze and Monitor Network Traffic.** Analyze high-volume network traffic to identify and monitor patterns consistent with robocalls. Company has set up a recurring schedule for conducting a comprehensive network monitoring plan with the goal of identifying irregular calling patterns that may indicate potential illegal originating robocalls. The schedule and areas of the network being monitored for illegal originating robocalls are outlined below:

a. Tandem Monitoring:

- Company has established a routine process of monitoring call quantity and patterns for originating traffic sent over the tandem trunk groups. By monitoring this traffic over an extended period of time, Company has established a baseline for traffic patterns based on their subscriber's regular usage. If Company notices spikes or changes greater than their predefined engineered threshold per trunk group, further analysis is conducted to identify the source of the change.
- This monitoring is conducted on a weekly basis for this portion of the network.
- If Company's monitoring process identifies the potential of illegal robocalls originating from the network, Company will follow the internal policy and procedure in accordance with this Program.

b. Local Monitoring:

- Company has deployed local monitoring tools based on the capabilities of the Class 5 switch. The Class 5 switch statistics allow Company to monitor originating traffic for all trunk groups or traffic to a particular carrier. The data collected is able to provide reports that can include total originating calls and total originating call usage. By monitoring this traffic over an extended period of time, Company has established a baseline for traffic patterns based on their subscriber's regular usage. If Company notices spikes or changes greater than their predefined engineered threshold per trunk group, further analysis is conducted to identify the source of the change.
- This monitoring is conducted on a weekly basis for this portion of the network.
- If concerns are identified for any individual line or MLTS, usage statistics can be used to further monitor that particular subscriber's service specifically. Company can set up reports to monitor originating call attempts and originating call usage. This data can help set a baseline of normal traffic patterns and signal when abnormal traffic patterns are emerging in order to further investigate.
- If Company's monitoring process identifies the potential of illegal robocalls originating from the network, Company will follow the internal policy and procedure in accordance with this Program.

c. Call Record Monitoring:

- Company utilizes a third-party billing vendor to process call detail records on a nightly basis by exporting the data from the Class 5 switch. These call records can be used to help identify the potential of illegally originating robocalls. If Company becomes concerned with any subscriber based on the collective and comprehensive efforts identified in this Program, the call records can be analyzed and summarized by the third-party billing vendor to flag traffic that has the characteristics of illegal originating robocall traffic. The monitoring includes high call volumes, low duration calls, sequential dialing patterns, calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator and other evolving best practices as identified by the collective industry helping to combat identifying illegal robocalls.

- This monitoring is conducted on an as needed basis for specific subscribers suspected of illegally originating robocalls.
- h. Investigate Suspicious Calls and Calling Patterns. Taking appropriate action to identify any party that is suspected of illegal robocalling or spoofing over its network.
- i. Company has explored partnerships with third-party validation service providers that use analytics to identify the origination or termination of illegal robocalls. The Company uses Industry Traceback Group's Do Not Originate list which provides a list of numbers for which the subscriber to the number has requested blocking.

Know-Your-Upstream Provider

- j. 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 of the Company's upstream providers. Going forward, all interconnection agreements will include prohibited traffic and traceback language.