

Robocall Data Mitigation Plan
ELLSWORTH COOPERATIVE TELEPHONE ASSOCIATION

FRN: 0005-0498-95

Filing Date: February 8, 2024

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

47 CFR § 64.6304a) – Non-IP networks allows 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:

Traceback Requests

- a. Pursuant to 47 CFR § 64.6305(B)(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 setup 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. Analyze and Monitor Network Traffic. Analyze high-volume network traffic to identify and monitor patterns consistent with robocalls.
- g. Investigate Suspicious Calls and Calling Patterns. Taking appropriate action to identify any party that is suspected of illegal robocalling or spoofing over its network.
- h. Company has explored partnerships with third-party validation service providers that use analytics to identify the origination or termination of illegal robocalls. Company is utilizing a caller authentication service. Within its service areas Company is utilizing Aureon, an end-to-end technology solutions organization, that provides a Caller Identification Authentication (CIDA) service which includes Outbound Shield technology. This Outbound Shield uses a curated list of high-risk phone numbers and detects invalid numbers. If the calling number has been reported as spam, the calling number will be prevented from completing outbound calls.

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