

# Robocall Data Mitigation Plan

## EON TELECOM INC.

The following documentation is to serve as the Robocall Mitigation Program of EON TELECOM INC. and their ongoing compliance with the Traced Act.

### **EON TELECOM INC hereby certifies the following information:**

EON TELECOM INC has committed to a Robocall Mitigation Program consistent with 47 CFR § 64.6305 for all originating calls made from its network.

EON TELECOM INC. (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 EON TELECOM INC. transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

### **EON TELECOM INC. hereby certifies to the implementation of the following practices:**

#### Traceback Requests

- a. Pursuant to 47 CFR § 64.6305(d)(4)(v), EON TELECOM INC. has designated a point of contact to receive notice of any incidents of illegal robocall traffic. The 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. EON TELECOM INC. 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 Processes

- c. EON TELECOM INC. will vet the identity of residential, retail, and wholesale subscribers through normal business practices and will obtain service address information.
- d. EON TELECOM INC. 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 Processes

- e. A subscriber is permitted to use a telephone number as their caller identity, if a number is directly managed by EON TELECOM INC. and/or obtained by EON TELECOM INC. via an underlying partner. EON TELECOM INC. has established a process established as 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, EON TELECOM INC. 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. EON TELECOM INC. has explored partnerships with third-party validation service providers that use analytics to identify the origination or termination of illegal robocalls. EON TELECOM INC. is utilizing a caller authentication service with an advance end-to-end technology solutions 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 EON TELECOM INC. 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.