

**Eastern Slope Rural Telephone Association
Strasburg Telephone Company
Eastern Slope Technologies, LLC**

ROBOCALL MITIGATION PROGRAM

Table of Contents

Table of Contents	2
I. PURPOSE OF THIS PROGRAM	3
II. DEFINITIONS	3
III. STATEMENT OF POLICY AND DESIGNATIONS	4
IV. GENERAL POLICIES FOR ROBOCALL MITIGATION	5
A. Requirements of Company to Mitigate Illegal Robocalls	5
B. Legal vs. Illegal Robocalls	5
V. PROCEDURES FOR ROBOCALL MITIGATION	6
A. Contact	6
B. Traceback	6
C. Subscriber Vetting – New and Renewing Customers	7
D. Service Agreements – New and Renewing Customers	7
E. Know-Your-Upstream-Provider	8
F. Telephone Number Validation	8
G. Network Capacity Limitations	8
H. Network Monitoring Call Analytics	9
I. Third-Party Call Analytics Services	10
J. International Call Originators	11
K. Certification and Contact Updates	11
APPENDIX 1 Third-Party Call Analytics Service	12

I. PURPOSE OF THIS PROGRAM

Eastern Slope Rural Telephone Association, on behalf of itself as well as any parent, brother/sister organization, and wholly owned subsidiaries (jointly, “the Company”), established a Robocall Mitigation Program (Program), implementing the policies and procedures within this Program for the reduction of the origination of illegal robocalls. In addition to these policies and procedures, the Company commits to cooperating with the Federal Communications Commission (FCC), law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that it learns are using its service to originate calls.

II. DEFINITIONS

Frequently used terms throughout this Program shall be defined as follows, in conjunction with any and all definitions as identified in 47 CFR § 64.6300.

Customer: A service provider’s subscriber, which may or may not be the ultimate End User of the telecommunications service.

End User: The entity ultimately consuming the telecommunications service and may include the End User’s device used for placing the call.

Foreign Voice Service Provider: Any entity providing voice service outside the United States that has the ability to originate voice service that terminates in a point outside that foreign country or terminate voice service that originates from points outside that foreign country.

Industry Traceback Consortium: The consortium that conducts private-led efforts to trace back the origin of suspected unlawful robocalls as selected by the Commission pursuant to §64.1203.

Robocall Mitigation Database: A database accessible via the Commission's website that lists all entities that make filings pursuant to §64.6305(b).

Telecommunications Carrier: a person or entity that meets the definition of 47 U.S.C. 1001(8), including a person or entity that FCC finds that its service is a replacement for a substantial portion of the local telephone exchange service under 47 U.S.C. § 1008(B) (ii).

Voice Service: Any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American Numbering Plan (NANP) or any successor to the North American Numbering Plan adopted by the Commission under section 251(e)(1) of the Communications Act of 1934, as amended; and includes:

(I) Transmissions from a telephone facsimile machine, computer, or other device to a telephone facsimile machine; and

(ii) Without limitation, any service that enables real-time, two-way voice communications, including any service that requires Internet Protocol-compatible customer premises

equipment and permits out-bound calling, whether or not the service is one-way or two-way voice over Internet Protocol.

This includes common carrier voice, interconnected Voice over Internet Protocol (VoIP), one-way VoIP, fax transmissions, and over-the-top voice services.

III. STATEMENT OF POLICY AND DESIGNATIONS

It is the policy of this Company to comply with the letter and spirit of all laws of the United States, applicable state statutes, and rules and requirements of the FCC. The Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) requires a voice service provider to implement robocall mitigation strategies to reduce the origination of illegal robocalls, including implementing the STIR/SHAKEN caller ID authentication technology in the IP portions of their phone networks as well as developing non-IP caller ID authentication solutions.

The FCC has issued orders requiring all voice service providers file certifications and Robocall Mitigation Programs to the Robocall Mitigation Database. These regulations require that voice service providers create policies and procedures that can “reasonably be expected to significantly reduce the origination of illegal robocalls.” As a part of its Robocall Mitigation Program, each service provider must:

- (i) Detail the “reasonable steps” it is taking to avoid originating illegal robocalls;
- (ii) Detail the procedures in place for its “new and renewing customer”
- (iii) Detail the procedures in place to “know-your-upstream provider”
- (iv) Detail if call analytics systems are used to identify and block illegal traffic
- (v) Commit to responding to traceback requests within twenty four (24) hours and cooperate with investigating and stopping illegal robocalls; and
- (vi) File its Robocall Mitigation Program in the Robocall Mitigation database.

This Program constitutes the required policies and procedures to implement this Company’s Robocall Mitigation Program. All officers, employees, or agents of the Company are required to follow the policies and procedures specified in this Program.

Robocall Mitigation Database Eligibility

The Company is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

STIR/SHAKEN Implementation Extension

The FCC granted an extension for the deadline to implement Caller ID authentication for providers falling within specified categories. Company qualifies for such extension pursuant to the following:

- §64.6304(d) – Non-IP networks. Those portions of a voice service provider’s 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.

Role in the Call Chain

Company has identified their role or roles in the call chain as part of the certification submitted within the Robocall Mitigation Database. The Company has outlined their robocall mitigation steps it undertakes for each role, if different, within this program.

IV. GENERAL POLICIES FOR ROBOCALL MITIGATION

A. Requirements of Company to Mitigate Illegal Robocalls

All officers, employees, and agents of the Company understand and agree that they will follow strictly the applicable federal and state laws, court orders, FCC Regulations, and Company’s policies and procedures in carrying out the responsibilities as described in this Program.

B. Legal vs. Illegal Robocalls

Voice Service Providers are required to take reasonable steps to avoid originating illegal robocall traffic, as defined within the Telephone Consumer Protection Act (TCPA).

Pursuant to the TCPA, and for purposes of this Program, an illegal robocall is a call:

- To a landline that leaves a pre-recorded or artificial voice message for telemarketing purposes, without a customer’s prior consent.
 - o Non-telemarketing calls to landlines, regardless of whether it is pre-recorded or an artificial voice message, are not considered illegal robocalls.
- To a wireless phone that leaves a pre-recorded or artificial voice message, or is made with autodialer equipment, without the customer’s prior consent.
 - o Calls to wireless phones do not need to be telemarketing in nature to constitute an illegal robocall; any telemarketing or information call made using the mechanisms above, and without prior consent, constitute an illegal robocall.

Company will implement its Program policies and procedures in an effort to reduce perceived illegal calls of the above types. If a customer claims that a call has been incorrectly flagged as an illegal robocall, the customer can notify Company for a more in-depth determination as to the legality of the call(s) in question.

V. PROCEDURES FOR ROBOCALL MITIGATION

A. Contact

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 Point of Contact is named in the Robocall Mitigation Database.

B. Traceback

Company will commit to respond, within twenty four (24) hours, to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating illegal robocallers that use its service to originate, carry, or process illegal robocalls.

When Company receives a notification of an illegal robocall originating from the Company's network, the following actions will be initiated:

1. Company personnel will review the call information to determine whether the call is from Company's network or one of its affiliates. If the call is from an entity other than Company, the notice will be forwarded on to that entity for review and any action or response.
2. If the call is from one of Company's customers in its network, Company personnel will attempt to identify the user. The following actions may be taken with offenders:
 - a. If the offender is an employee, the responsible supervisor will be notified, and appropriate disciplinary action may be warranted. A copy of the violation will be filed by HR in the employee's personnel file.
 - b. If the offender is a customer, the customer will be notified by telephone and email of the offense. If it is a first-time offense, the customer will be notified and advised that an alleged violation has been received and that any further violations could affect the customer's account. Notification of a second offense will result in the same action. A third offense will result in notice that the customer's service has been restricted for ninety (90) days to limit the ability to violate the law. A fourth offense will result in termination of service.

In addition to the above actions Company may take when it identifies a pattern consistent with illegal robocalls, Company may also initiate or cooperate in a traceback investigation to verify that the originating customer owns or is authorized to use a Caller ID number. In

conjunction with following Industry Traceback Group-recommended best practices, Company has sufficient resources to promptly respond to traceback and trace forward investigations.

Upon receipt of notice from Company that an illegal robocall originated from customer's number, customer may dispute the determination.

1. If the customer's number has been inadvertently flagged as illegal robocalling due to third-party unauthorized spoofing of the customer's number, Company will make a good faith effort to contact database vendors in an attempt to correct the issue.
2. If the robocall was a legal robocall originating from the customer, the circumstances of the robocall will be reviewed with the customer and the customer will be monitored for a thirty (30) day period thereafter.

C. Subscriber Vetting – New and Renewing Customers

Company has implemented know-your-customer processes to stop illegal calls before they are placed. 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:

- (i) physical business location;
- (ii) a contact person for the business;
- (iii) state or country of incorporation; and/or
- (iv) federal tax ID.

Company will complete an additional review of any outbound call centers or high-volume origination services within its network, including more stringent background checks and site visits as needed.

D. Service Agreements – New and Renewing Customers

Company maintains a document outlining the acceptable uses of the service and prohibits among other things:

- (i) modification of network information for deceptive purposes;
- (ii) violation of local, state, or federal laws; and
- (iii) use of Company's network to engage in fraudulent activity.

Company reserves the right to suspend or terminate any subscriber account for violating the service terms. Company will also require a point of contact which can be contacted if needed for traceback cooperation in case illegal robocalling is detected.

E. Know-Your-Upstream-Provider

Company knows all the carriers from which it sends or receives traffic. The Company will monitor the status of these carriers within the Robocall Mitigation Database and will not accept traffic from those carriers that are removed. In addition, the filed Programs of these carriers have been reviewed by the Company to understand the specific steps a provider is taking to mitigate illegal robocalls. These steps and others outlined within this Program help mitigate the possibility of immediate upstream providers using the Company to carry or process a high volume of illegal traffic.

F. Telephone Number Validation

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. For both single line services and MLTS, this screening conducted by each Class 5 switch allows for an automated and secure means of validating all originating telephone numbers. With validating and accepting only assigned or approved numbers are being used by the originating calling party, Company can fully cooperate with traceback efforts. If Company has a subscriber that requires to originate a number that has not been assigned to them, Company requires a Letter of Authorization (LOA) that they are the authorized user of the number to validate and authorize its use before allowing it to be originated on the network.

G. Network Capacity Limitations

The Company has reviewed the network capacity requirements for the two primary segments of the network, subscriber facing and PSTN facing, and has established appropriate capacity limitations to align with each service need. By limiting the capacity of each segment of the network based on service needs allows Company to mitigate the risk of flooding the network with unintended calls, such that it is appropriately sized to minimize call blocking, but not allow excess calling capability that could be used to generate illegitimate traffic. These efforts protect both on-network and off-network subscribers to be able to traceback originating calls to their source.

For the subscriber facing segment of the network, when a new service is established the capacity requirements are discussed with each subscriber. For example, if providing service to a MLTS, the concurrent call capacity is determined by understanding the subscribers service needs such as how many end points will be used, average call usage and other metrics. This allows Company to establish connectivity to MLTS that is right sized based on the subscribers need. This connectivity is capped by the Class 5 switch so no more concurrent calls than the identified number can originate. This concurrent call capacity is monitored and can be expanded by the subscriber when the service need is identified. In addition to limiting the capacity of originating calls for MLTS, Company also limits the number of concurrent calls for individual lines based on the service need. This is accomplished within the Class 5 switch by restricting the number concurrent calls of each end point to the original subscriber service request. Similarly, this will not allow an unintended number of calls to originate from a subscriber.

For the PSTN facing segment of the network, all connections to tandem switches, other service providers and interexchange carriers are limited to a concurrent call capacity sufficient to limit call blocking, but not grossly oversized to allow for opportunity to flood the PSTN with illegitimate traffic. These capacity limits are set on both trunk groups regardless of technology and are scaled back or expanded when thresholds for the trunk capacity are reached.

H. Network Monitoring Call Analytics

Company has setup 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:

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.

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.

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 illegal 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 illegal originating robocalls.

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.

I. Third-Party Call Analytics Services

Company has explored partnerships with third-party call analytics service providers that use analytics to identify the origination of illegal robocalls. If Company has elected to utilize a third-party call analytics service to monitor originating traffic as a mitigation tool, a description of the service is outlined in Appendix 1. If originating traffic is flagged as potential robocall traffic, Company follows internal policy and procedure in accordance with Section V of this Program.

J. International Call Originators

Company is not currently a Foreign Voice Service Provider but if the Company does sell its services to international call originators using North American Numbering Plan numbers it will develop processes to validate that the calling party is authorized to use the telephone number or caller identity.

K. Certification and Contact Updates

As required, the Company will submit any necessary updates because of changes to Company certification, identification information, or contact information to the Commission within 10 business days of the change.

APPENDIX 1
Third-Party Call Analytics Service

Company has not partnered with a third-party call analytics service. Company has leveraged the best practices outlined in this Program to combat illegal robocalls.