

NORTH ALABAMA ELECTRIC COOPERATIVE

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. Third-Party Network Provider	8
G. Third-Party Call Analytics Services	8
H. International Call Originators	9
I. Certification and Contact Updates.....	9
J. Do-Not-Originate.....	9

I. PURPOSE OF THIS PROGRAM

North Alabama Electric Cooperative, 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. Company has partnered with Crosstel Tandem, Inc. (“Third-Party Network Provider”), to provide the voice services to their subscribers and lacks control of the necessary network infrastructure to implement STIR/SHAKEN. However, Company understands the importance of a ubiquitous approach of all parties involved with delivering voice services to combatting illegal robocalls. This program outlines the reasonable steps being performed for robocall mitigation, at least to the extent that they are able, despite their lack of control over network infrastructure. 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).

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. Company lacks control of the necessary network infrastructure to implement STIR/SHAKEN themselves but has partnered with a third party that has implemented the STIR/SHAKEN caller ID authentication technology in the IP portions of their voice networks as well as developing non-IP caller ID authentication solutions.

The FCC has issued orders requiring all voice service providers to 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(b) - Voice service providers and gateway providers that cannot obtain an SPC token. Voice service providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6301 until they are capable of obtaining a SPC token. Gateway providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6302(c) regarding call authentication.

In addition, Company is unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN.

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 and is listed as a “Voice service provider without a STIR/SHAKEN obligation”. The Company has outlined the robocall mitigation steps it undertakes within this program and can still support lacking control of the network infrastructure.

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 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 work with their Third-Party Network Provider to 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 or its Third-Party Network Provider 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; and
- (iii) 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 (eg. Acceptable User Policy (AUP), Tariff, etc.) 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 lacks control of the necessary infrastructure to have direct interconnections with other carriers and has partnered with a Third-Party Network Provider that facilitates the connectivity to upstream providers. Company has reviewed and confirmed their Third-Party Network Provider has filed in the Robocall Mitigation Database and reviewed their Robocall Mitigation Program. The Company will monitor the status of their Third-Party Network Provider's Robocall Mitigation Database status and will move services to a different partner if the current Third-Party Network Provider is removed from the Robocall Mitigation Database. 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. Third-Party Network Provider

Company has partnered with a Third-Party Network Provider, to provide the voice services to their subscribers and Company lacks control of the necessary infrastructure to implement STIR/SHAKEN and network based robocall mitigation best practices. While Company lacks the control to implement these critical network functions, the Third-Party Network Providers ability to effectively perform these functions is a foundation of the continued relationship.

The Third-Party Network Provider maintains the primary role of the following functions to assist in meeting network based robocall mitigation compliance.

- Network Monitoring
- Traffic Management
- Knowing their Upstream Providers
- Alerting of Robocall Activity
- Call Analytics

In addition to the above robocall mitigation steps, the Third-Party Network Provider has a Complete STIR/SHAKEN Implementation status and has fulfilled their own obligations with Robocall Mitigation Database Certification and Program filing.

G. Third-Party Call Analytics Services

Company lacks control of the necessary network infrastructure to implement a Call Analytics solution themselves. However, Company has partnered with a Third-Party Network Provider who has filed in the Robocall Mitigation Database and their filed Robocall Mitigation Program details the Call Analytics solution and vendor for monitoring network traffic. If Company is notified of traffic that is flagged as potentially illegal robocall traffic from their

Third-Party Network Provider, Company follows internal policy and procedure in accordance with Section V of this Program.

H. 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.

I. 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.

J. Do-Not-Originate

As part of the Company's ongoing efforts to prevent illegal robocalls and to comply with FCC requirements, Company has confirmed with their Third-Party Network Provider that Do-Not-Originate call blocking measures are in place.