

Coon Rapids Municipal Communications Utility

ROBOCALL MITIGATION PROGRAM

Version 2/2024

STATEMENT OF POLICY AND DESIGNATIONS

It is the policy of this Provider to comply with applicable statutes 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 Provider’s Robocall Mitigation Program. All officers, employees, or agents of the Provider are required to follow the policies and procedures specified in this Program.

Robocall Mitigation Database Eligibility

The Provider 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. Provider 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

Provider contracts with a third-party wholesaler, Northwest Iowa Telephone Company, identified under RMD0002534, and located in Sergeant Bluff, Iowa. Provider has identified their role in the call chain as part of the certification submitted within the Robocall Mitigation Database. The Provider has outlined their robocall mitigation steps, alongside the wholesaler's process in wholesaler's Robocall Mitigation Plan.

GENERAL POLICIES FOR ROBOCALL MITIGATION

A. Requirements of Provider to Mitigate Illegal Robocalls

All officers, employees, and agents of the Provider understand and agree that they will follow strictly the applicable federal and state laws, court orders, FCC Regulations, and Provider'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.

Provider 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 Provider for a more in-depth determination as to the legality of the call(s) in question.

PROCEDURES FOR ROBOCALL MITIGATION

A. Contact

Pursuant to 47 CFR 64.6305(B)(4), the Provider has designated a point of contact to receive notice of any incidents of illegal robocall traffic. This Point of Contact is:

Brad Honold at 712-999-2225 and email brad.honold@crmu.net

B. Traceback

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

1. Provider personnel will review the call information to determine whether the call is from Provider's network.
2. If the call is from one of Provider's customers in its network, Provider personnel will attempt to identify the user. The following actions may be taken with offenders:
 - 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.
 - A second 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 third offense will result in termination of service.

In addition to the above actions Provider may take when it identifies a pattern consistent with illegal robocalls, Provider, with its third-party wholesaler, 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. Upon receipt of notice from Provider that an illegal robocall originated from customer's number, customer may dispute the determination.

1. 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

Provider has implemented know-your-customer processes to stop illegal calls before they are placed. Provider will vet the identity of retail 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, Provider 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) federal tax ID; and/or
- (iv) nature of customer's business.

Provider 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

Provider maintains a document (e.g., 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 Provider's network to engage in fraudulent activity.

Provider reserves the right to suspend or terminate any subscriber account for violating the service terms. Provider 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

Due to the rurality of the parties, Provider's third-party wholesaler knows all the carriers from which it sends or receives traffic. Wholesaler commits to monitor the status of these carriers within the Robocall Mitigation Database and will not accept traffic from those carriers that are removed. These steps and others outlined within this Program help mitigate the possibility of immediate upstream providers using the Provider to carry or process a high volume of illegal traffic.

F. Network Monitoring Call Analytics

Provider's wholesaler has established the ability for conducting a comprehensive network monitoring when required to identify irregular calling patterns that may indicate potential illegal originating robocalls.

Tandem Monitoring:

Wholesaler has established a process for monitoring call quantity and patterns for originating traffic sent over the tandem trunk groups. If illegal robocalling is suspected, these monitoring tools will be employed to monitor traffic patterns. As part of this monitoring, if wholesaler notices spikes or changes greater than their predefined engineered threshold per trunk group, further analysis is conducted to identify the source of the change. If the monitoring process identifies the potential of illegal robocalls originating from the network, wholesaler and Provider will follow the internal policy and procedure in accordance with this Program.

Local Monitoring:

Wholesaler has deployed local monitoring/diagnostics tool based on the capabilities of the Class 5 switch. The Class 5 switch statistics and troubleshooting software allows

wholesaler to monitor all originating traffic. The data collected is able to provide reports that can include total originating calls, total originating call usage, call traces, and more. These tools are able to monitor traffic for calls that have been placed in the previous days or weeks. As part of this monitoring, if wholesaler notices spikes or changes greater than their predefined engineered threshold per directory number, further analysis is conducted to identify the source of the change. If concerns are identified for any individual line or MLTS, usage statistics and network monitoring software can be used to further monitor that particular subscriber's service specifically. Wholesaler currently utilizes daily reports to monitor originating call attempts and originating call usage. If wholesaler's monitoring process identifies the potential of illegal robocalls originating from the network, Provider will be notified, and parties will follow the internal policy and procedure in accordance with this Program.

Call Record Monitoring:

Provider's wholesaler 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 Provider or wholesaler 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.

Wholesaler has deployed a monitoring/diagnostics tool as part of their Class 5 switching network. This diagnostics tool provides detailed call traces suitable for Provider to diagnose, monitor and collect data associated with calls traversing the network. When the monitoring/diagnostics tools are enabled on the switching system, traces are recorded for all calls and transferred to an external database for future review. These traces do not have to be individually enabled on particular lines or subscribers and are always active. When investigating suspicious traffic, a web application is used to search the database for traces for particular lines or subscribers and to view the traces. The application also allows traces to be printed or exported for offline storage for further evaluation if required. The traces include decoded signaling messages, routing, and number validation events, call service actions/decisions, codec selection, echo cancellation programming, media events such as digit and tone detection, tone generation, and digit out-pulsing, billing records and concise call logs. This collection of data allows for a comprehensive ability to monitor network traffic.

This monitoring is conducted on an as needed basis for specific subscribers suspected of illegal originating robocalls.

If wholesaler's monitoring process identifies the potential of illegal robocalls originating from the network, Provider will be contacted and parties will follow the internal policy and procedure in accordance with this Program.

G. Third-Party Call Analytics Services

Provider and its wholesaler have explored partnerships with third-party call analytics service providers that use analytics to identify the origination of illegal robocalls. If Provider 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, Provider and wholesaler will follow internal policy and procedure in accordance with this Program.

H. International Call Originators

Provider is not currently a Foreign Voice Service Provider but if the Provider 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 Provider will submit any necessary updates because of changes to Provider certification, identification information, wholesaler, or contact information.

APPENDIX 1

Third-Party Call Analytics Service

Beyond what is stated above, Provider has not partnered with a third-party call analytics service. Provider has leveraged the best practices with its wholesaler, Northwest Iowa Telephone Company, as outlined in this Program to combat illegal robocalls.