

The Community Agency of O'Brien County

Robocall Mitigation Plan

Updated 2/2024

DJ Weber, General Manager at 712-930-5593

This Robocall Mitigation Plan is submitted by The Community Agency of O'Brien County (TCA) pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission (FCC) which require all "voice service providers" to establish a "robocall mitigation plan". This document sets forth the Provider's current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. The Provider views these policies and procedures as constituting "reasonable steps" to avoid the origination of illegal robocalls on its network and in addition to following these steps the Provider commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

I. STIR-SHAKEN IMPLEMENTATION STATUS

As indicated in the FCC's Robocall Mitigation Database, the Provider's status with respect to STIR-SHAKEN implementation is as follows:

Presently, the Provider relies on the continuing extension from STIR-SHAKEN implementation provided under 47 CFR § 64.6304 (d) which exempts from STIR-SHAKEN Caller ID Authentication those portions of a voice service provider network that rely on technology that cannot initiate, maintain, carry, process, and terminate SIP. Provider relies solely on contracted wholesaler's facilities, Thinq dba Commio, which are IP and capable of initiating, maintaining, carrying, processing, or terminating SIP calls which include STIR-SHAKEN attestation data.

TRACEBACK REQUESTS

As noted above, the Provider will cooperate with the FCC, law enforcement and the (ITG) on all traceback requests and investigations. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, the Provider will dedicate sufficient resources to promptly complete and provide responses to all traceback requests received from the FCC, law enforcement and/or the ITG, and commits to fully responding to any traceback request received within 24 hours after receiving the same. Within **Appendix A** to this Plan, the Provider identifies a single point of contact for receiving all traceback requests.

As part of its efforts to assist in the successful traceback of illegal robocalls, the Provider will going forward include within its carrier interconnection and/or service agreements language requiring traceback cooperation on any voice service calls exchanged. In part, these related

contract provisions will specify the need for parties to promptly identify the upstream provider from which a suspected illegal robocall entered its network or the customer of the service from which the call originated.

II. CUSTOMER VETTING PRACTICES

As a means of preventing or minimizing the origination of illegal robocalls through its voice services, the Provider will use best practices in vetting the identity of all of its voice service subscribers, whether a retail or business/commercial subscriber (including any entities that are purchasing the Provider's services for resale). The subscriber vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a service relationship. Generally, the Provider looks to confirm the identify of customers using its voice services through collecting information such as physical customer location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer's business. Provider efforts to vet retail and business/commercial subscribers occurs during the process of provisioning customer requested services (for example in appropriately sizing the facilities to their claimed intended use), executing the Provider's required service agreements, and granting the customer the right to use telephone number resources. Commercial end users, comprised of larger businesses with more complex service configurations, are generally recognized as presenting a higher risk of perpetrating illegal robocalls and thus those customers, at the Provider's discretion, may be subject to an additional review, including a more stringent background check and possibly a site visit. The Provider also understands the special importance of vetting any wholesale customers it may have. If necessary, the Provider may vet identity information for its wholesale customers by confirming whether the customer is an FCC Form 499-A filer in the FCC Form 499-A Filer database or in the FCC's Intermediate Provider Registry. If the customer is not registered within those databases further investigation is conducted to better understand the nature of the customer's business.

Further, with respect to meeting existing obligations to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls, the Provider:

Utilizes service agreements and acceptable use policies as a means of preventing its new and existing subscribers from using their voice and broadband services in ways that would be in violation of local, state, or federal laws, or to engage in deceptive or fraudulent activity. These documents governing use of Provider provided services include terms indicating specifically to all customers that their services should not be used for the purpose of making illegal robocalls, and the Provider reserves authority within its service agreements to suspend or terminate a subscriber's voice service for violating applicable service-related terms.

- Has established a routine process for monitoring of the usage and quality of its network facilities and conducts recurring and timely reviews of its call detail records (CDRs) to

facilitate early identification of unusual or suspicious calling activity or patterns that may indicate use of the network for originating illegal robocalls. In those instances where the Provider identifies activity or a pattern consistent with illegal robocalls the customer will be contacted within one business day for further investigation and possible action regarding their subscribed to voice service.

III. TELEPHONE NUMBER VALIDATION PRACTICES

Telephone Number Validation refers to the confirmation of the customer or end-user right to use a telephone number in connection with their subscribed voice service(s). In accord with industry best practices, the Provider has procedures in place to confirm the calling customer's right to use a telephone number. Specifically, a subscriber of the Provider's services is permitted to use a telephone number as their caller identity if a number is directly managed by the Provider and/or obtained by the Provider via an underlying partner.

V. KNOW YOUR UPSTREAM PROVIDER PROCEDURES

As a rural provider of voice services, the number of upstream providers used by the Provider to receive and deliver its originated voice calls for termination are somewhat limited. The Provider has longstanding relationships with these upstream providers and maintains its awareness of the nature of their businesses and the legitimacy of their call transmission services. Further, the Provider, in the interest of providing the highest quality services to all of its voice service customers, is committed to taking those steps necessary to ensure that any upstream providers providing connectivity are equally committed to monitoring their networks and preventing their use for the transmission of illegal robocalls. This includes the use of robocall prevention language in any contracts that the Provider may directly have with any upstream provider entities. Included as part of **Appendix A** to this Robocall Mitigation Plan document is a list of the Provider's current, immediate "Upstream Provider(s)" along with contact information for each.

VI. ONGOING ROBOCALL MITIGATION PRACTICES

The Provider monitors the usage of its network and examines call detail records (CDRs) on a recurring basis for the purpose of detecting suspicious call activity and/or calling patterns. When network usage patterns consistent with illegal robocalls are detected or the Provider otherwise suspects illegal robocalling or spoofing is taking place on its network, it immediately seeks to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action. The actions taken may include, but are not limited to: initiating a traceback investigation; verifying that the originating customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's corporate name, trademark, or d/b/a name;

terminating the party's ability to originate, terminate, or route calls on the Provider's network; and providing notice to law enforcement authorities.

As part of its Plan to mitigate and prevent any originating robocalls on its network, the Provider is committed to early identification and investigation of possible robocalling situations. In monitoring usage of its network, particular attention is given to: (1) higher than normal subscriber traffic volume including large bursts of traffic in small timeframes or inconsistent volumes of traffic (spikes in usage); (2) originating calls of short duration and low call completion percentages; (3) originating calls with sequential called to number dialing patterns; (4) repeated calls made to do-not-call registry or invalid numbers; and (5) calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator.

VII. THIRD-PARTY CALL ANALYTICS

The Provider also uses third-party call analytics, described below, to further assist and prevent the origination of illegal robocalls on its network. Included in **Appendix A** is the name of the vendor(s) used along with a description of the call analytics system(s) used to identify and block illegal robocall traffic.

Appendix A

Traceback Request Single Point of Contact:

Name: D.J. Weber

Title: GM

Phone Number: 712-930-5593

Email Address: djweber@tcaexpress.net

Upstream Provider Information:

Name of Upstream Provider: Aureon

Nature of Business: Tandem Switch Provider; Wholesale Long-Distance Provider

Network Location of Upstream Provider: West Des Moines, IA

Contact: NOC

Phone Number: 800-588-4082

Second Upstream Provider – Commio

Wholesale LD Provider

5420 Wade Park Blvd.

Suite 100

Raleigh, NC 27607

Phone: 919-890-0000

<https://www.commio.com/contact/>

support@thing.zendesk.com

Call Analytics Vendor Name and Description of System:

Name of Vendor (RVW)

Call analytics purchased from the vendor determine if originating calls should be blocked. If the telephone number appears on a Do-not-call list or otherwise is an unallocated, unused, or invalid number, the call will be determined to be fraudulent and needs to be blocked. Vendor may also use advanced fraud detection which enables behavior analysis and tracking of abnormal and unexpected calling patterns to detect high volume robocalling, spoofing, and suspicious call activity.

Description of analytics - Company's switch pushes files to an ftp site that RVW can access twice a day at roughly 1:00 a.m. CDT and 1:00 p.m. CDT.

RVW downloads the files around 8:00 a.m. CDT each business day. Weekend and holiday files are processed on the next business day.

Each business day, RVW converts the switch files into a standardized RVW LAMA format.

During this conversion, call patterns are monitored, and suspicious call patterns are identified. These will be originating calls from a single telephone number which exceed established thresholds based on prior usage. RVW can then run additional analysis on the data and produce detailed reports which include the originating and terminating numbers along with call times and call duration. These detailed reports are then forwarded to the General Manager and CO Manager for further investigation.

RVW realizes that at times, schools, civil defense and other organizations may make mass callings that we are not aware of. This calling would also be forwarded to the General Manager and CO Manager for further investigation.