

CONTERRA ULTRA BROADBAND, LLC – d/b/a Conterra Networks
DETEL WIRELESS, LLC
Robocall Mitigation Plan V.3

STIR/SHAKEN Implementation

This Migration Plan covers Conterra Ultra Broadband, LLC and its affiliate, Detel Wireless, LLC (collectively, “Conterra” or “Companies”). This document details the reasonable steps and actions taken by Conterra to mitigate and eliminate illegal robocalling. The Companies have an ongoing commitment to scan for and help alleviate illegal robocalling by pre-qualifying prospective customers, monitoring existing customers for traffic patterns indicative of prohibited robocalls, and working with other providers and regulatory agencies in combatting fraudulent voice activity.

The Companies provide retail Voice over Internet Protocol (“VoIP”) calling services. These voice services are provided on a retail only basis. As telecom resellers that lack control over the network infrastructure necessary to implement STIR/SHAKEN, the Companies are exempt from a STIR/SHAKEN implementation obligation. See *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3241, para. 40; 47 CFR Section 64.6304(b).

Know Your Underlying Provider

The Companies have a master service agreement with Momentum Telecom and Alianza Communications and have received written assurances from their officials that they have and will continue to sign calls submitted to the Companies and will abide by the FCC’s STIR/SHAKEN and robocall mitigation rules in all respects when providing voice services to Conterra. The Companies and their upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests. Momentum Telecom and Alianza Communications use their tokens to sign calls on behalf of the Companies.

Know Your Customer

Screening interviews are performed to understand potential customer business models and the potential, or lack thereof, for involvement in fraudulent robocalling schemes. Conterra performs a credit check which may include a DUNS prior to providing any service.

In our research of potential voice customers, Conterra will not activate clients that provide anonymous information or where data mismatches are found. Additionally, prospective customers are required to agree to the Companies’ strict policies and contractual terms prohibiting the act of fraudulent voice activity as a condition of doing business with Conterra and a violation by a customer will lead to termination of services.

Individuals associated with prospective or current customers who have been known to act improperly or otherwise be involved in fraudulent robocalling will cause their companies to be rejected by Conterra as a customer and any existing customer relationships could potentially be severed.

Traceback Requests

The Companies will cooperate with all applicable regulatory and law enforcement agencies regarding all traceback requests and investigations. The Companies will dedicate sufficient resources to promptly complete and provide responses to all traceback requests received from law enforcement and regulatory agencies within 24 hours after receiving a request. As part of its efforts to assist in the successful traceback of illegal robocalls, the Companies will include within its carrier service or interconnection agreements language requiring traceback cooperation on voice service calls exchanged. Our point of contact to handle all traceback requests is included in Appendix A.

The Companies will assist with the mitigation of illegal activity when it has been notified by the Commission through its enforcement bureau. If illegal activity is confirmed, the Companies will exercise their rights under its Acceptable Use Policy and FCC orders to take the necessary actions to block illegal calls. The Companies has prepared an Acceptable Use Policy (“Policy”) as a guide for its customers to understand the intended and permissible uses of our service, and to prevent exploitation, fraud, and abuse of our unlimited calling plans and features. This policy is applicable to all our services and can be found at the following link: <https://www.conterra.com/acceptable-use-policy/>.

If a traceback exposes an existing customer as the source of fraudulent robocalls, or as having transmitted fraudulent robocalls, a demand for an explanation and verification of mitigation of the traffic is issued to the customer. If the fraudulent traffic is not remediated, Conterra and its affiliates immediately begins rejecting all traffic from the offending customer.

Telephone Numbers

A Telephone Number (“TN”) based caller identity is the originating phone number included in call signaling used to identify the caller for screening purposes that is uniquely associated with the subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by Conterra and/or obtained by the Companies from the Companies’ underlying carrier for use by the subscriber. Numbers can also be allocated by Conterra or ported using information from previous bill matching customer information.

International Calling

Conterra is not currently an international voice services provider. If at any time it does decide to sell services to international customers using North American Numbering Plan resources, we will familiarize ourselves with and develop best practices for full vetting of such customers and work with our underlying providers to perform the necessary telephone number validation on all international originated calls.

Call Analytics

As a reseller, Conterra must rely on its underlying providers and/or their third-party vendors to determine if originating calls should be blocked based on call analytics practices. Conterra has not contracted directly with a third-party vendor for call analytics.

Ongoing Robocall Mitigation

The Companies rely on third-party network providers to monitor and examine call detail records (CDRs) on a repeating basis to detect suspicious call activity and/or calling patterns. When we and/or our underlying providers detect network usage patterns consistent with illegal robocalls or suspect illegal robocalling is taking place, we will immediately seek to identify the party that is originating, terminating, or routing these calls so that we 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 and/or d/b/a name; block the party's ability to originate, terminate, or route calls on the network; and/or providing notice to law enforcement authorities.

As part of our Plan to mitigate and prevent any originating robocalls, we are committed to early identification and investigation of possible robocalling conditions. Among other things, we watch for higher-than-normal subscriber traffic volume, including large bursts of traffic in small timeframes or spikes in usage. We also monitor for originating calls of short duration and low call completion percentages, originating calls with sequential called to number dialing patterns.

Appendix A

Traceback Contact Information Name	Title	Contact Information
NOC	Network Operations Center	Ph: 1-800-634-1374 Email: noc@conterra.com
Bob Ziemba	Senior NOC Consultant	Ph: 903-323-4518 Email: bziemba@conterra.com
Dawna Hannan	VP HR and Telecom Regulatory	Ph: 704-936-1805 Email: dhannan@conterra.com

Contact for Robocall Mitigation-Related Issues

The Company will update its Robocall Mitigation filings within 10 business days of any change to the information outlined in this plan. Please direct any questions related to Robocall Mitigation issues to:

Dawna Hannan
VP HR and Telecom Regulatory
5301 77 Center Drive
Charlotte, NC 28217
Phone: 704-936-1805
dhannan@conterra.com