

Solarus Robocall Mitigation Policy

Robocall Mitigation Compliance with TRACED Act

Version: 3.1	Date: 2026-02-04	Updated By: Kurtis Bredda
--------------	------------------	---------------------------

I. Overview

The FCC requires all voice service providers to certify in the Robocall Mitigation Database their status for

compliance with STIR/SHAKEN and to certify to the implementation of a Robocall Mitigation Plan to ensure that illegal traffic does not originate on

their network(s).

This robocall mitigation plan is submitted on behalf of Wood County Telephone Company -OCN 0974 and Manawa Telephone Company – OCN 0905 both incumbent local exchange carriers d/b/a Solarus and its wholly owned subsidiary Central Wisconsin Communications – OCN 997C, a competitive local exchange provider. All companies operate in Wisconsin and share operations including their respective Robocall Mitigation Plans. The companies are collectively referred to as Solarus within this Robocall Mitigation Plan.

Solarus is eligible for the continuing extension of the STIR SHAKEN implementation deadline as a small voice service provider (§64.6304 (a)(2) that has non-IP portions within its network §64.6304(d).

Solarus provides local service to fewer than 100,000 voice subscriber lines. The majority of customers are served on the IP portions of the Solarus network which relies on technology that initiate, maintain, carry, process, and terminate SIP calls.

Solarus also originates calls via SIP connections within its network. Solarus has registered with the Policy Administrator and is an authorized service provider in the STIR|SHAKEN ecosystem. Solarus has implemented STIR|SHAKEN within its IP-network and signs the calls originating on the IP portions of the Solarus network.

All the voice traffic that originates on the Solarus network is subject to the robocall mitigation program described below.

II. General Terms and Conditions

Agreeing to the terms and conditions of Solarus's phone service commits the customer to abiding by the following Robocalling rules and restrictions.

Solarus prohibits activities normally associated with Robocalling including, but not limited to:

- Providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call.
- Violating any applicable local, state, or federal law; using the Solarus service to engage in or in connection with fraudulent activities.

Failure to abide by the aforementioned terms and conditions will result in termination of service and potential government intervention.

We will also update our Terms and Conditions agreement with our customers to include Robocall Mitigation policies and procedures.

III. Know Your Customer

Solarus utilizes several current methods of Robocall Mitigation within our own Switching Network to prevent unlawful robocalls from originating on our Network. We have traffic monitoring in place that will notify us of unusual behavior. In addition, our interexchange carriers will identify, notify, and block potential robocalling and other unusual telecommunications activities that originate on our Networks.

Residential phone lines are set to a “maximum simultaneous registration” number of 1. This prevents placing more than one call at a time from a single directory number (DN). We use SIP Authentication practices with strong passwords on our SIP/FTTH phone lines. This will help prevent multiple registrations and calls originating on our Networks.

- We follow the best practices for vetting caller identity described by the NANC Call

Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

1. Residential lines will only be able to place one call at a time and will only be able to place calls originating from their own phone number (since the number is supplied by our switch, not the access equipment).
2. Business lines will have similar limits. We will configure our switch to only accept calls from DNs they own (using Innovative Systems Terminating Call Management) and we have set up originating capacity limits on certain PBX/Business customers.
3. Traditional T1s/PRI's are limited to 24 and 23 calls at one time.
4. SIP Trunks are sold and limited to the number of lines requested by the business.

IV. Incorporation of Additional Tools and Measures for Mitigation

1. Solarus is partnered with Ribbon Communications, East Wind Communications, Innovative Systems, Equinix Information Systems and Next-Tech to incorporate Tools and Measures to alert Solarus to potential robocalls originating on our Network.,
2. Solarus has partnered with Ribbon Communications to implement STIR|SHAKEN and use their database and equipment.
3. We also employ many checks to make sure we minimize the abuse of Robo Calls being made to and from our network.
 - a. Solarus utilizes two solutions to combat on network originating ROBO Calls.
 - i. The first defense we utilize is the Next-Tel VQM. This gives us a daily report of all suspicious calls made the prior day. Suspicious includes long duration, High Call Volume, Short Call Duration coupled with High call volume and excessive repeat calls. These reports are reviewed by a technician every morning.
 - ii. The second defense against ROBO calls and Fraud is the Equinix Protector Solution. This solution monitors calls being originated on our switch. It evaluates the calls every 15 min and has rules put in place to disable any TN that is abusing our system. Our Engineers and NOC are notified when and if that happens.

4. If any calls are deemed suspicious the technician will investigate. If needed and appropriate the matter will be escalated to an Engineer to confirm. If deemed appropriate they will contact the customer. If the Customer refuses to stop the calls that are violating the service agreement this would be clear violation of the Solarus service agreement and the services will be terminated. If needed Law enforcement is notified.
5. When new customers apply for service, they will be asked for a Driver's license and Social Security Number. If it is a business account, then we will also ask for the Tax ID.
6. To help prevent our customers from receiving Robo calls we have implemented Innovative Systems Terminating Call Manager feature on our incoming company long distance trunks, we have been able to block or challenge telemarketing calls and spoofed calls. This feature allows us to add known telemarketers' numbers manually and it also auto updates weekly from the FCC's known telemarketers list. All telco customers have the option to add TCM to their individual line to allow them to control their incoming calls.

V. Investigation

Solarus promptly investigates calls identified as potential illegal robocalls or those that have abnormal call volumes, patterns or activity consistent with illegal robocalls.

In addition, if Solarus has any other reason to suspect illegal robocalling or spoofing is taking place over its network, Solarus will work internally to identify the party that is using our network to originate, route, or terminate such calls and take appropriate action.

VI. Upstream Provider Knowledge

Solarus knows all the carriers from which it receives traffic and has confirmed that all of the carriers are listed in the Robocall Mitigation Database. Solarus has also reviewed the connected carrier's RMPs to learn how the carriers monitor their originating traffic to mitigate illegal robocalls. In addition, Solarus is now incorporating traceback and prohibited traffic language in all contractual agreements with upstream carriers.

VII. Role In the Call Chain

Solarus is a voice service provider with a STIR/SHAKEN implementation obligation on the IP-Portions of its network. We are also a Tandem Provider and transit calls thru our network for other companies and carriers.

VIII. Robocall Mitigation Database Eligibility

Solarus has not been involved in any recent, formal law enforcement or regulatory investigation into suspected unlawful robocalling.

Solarus has not been prohibited from filing in the Robocall Mitigation Database (RMD).

IX. Traceback and Enforcement Cooperation

Solarus will respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls. Solarus will dedicate the needed personnel and resources to provide prompt and complete responses to Traceback requests. Solarus will respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium fully and in a timely manner within twenty-four (24) hours.