

Robocall Mitigation Plan

Robocall Mitigation Compliance with TRACED Act

Date	Organization	Change Summary
September 9th, 2021	ComTec Cloud Services LLC	Initial Version

Objective: Establish and follow a policy that is compliant with TRACED Act

Overview:

The FCC requires that all providers certify in the Robocall Mitigation Database their status for compliance with STIR/SHAKEN. Those not yet fully compliant must implement and certify to the implementation of a Robocall Mitigation Plan to ensure that this illegal traffic does not originate on their networks as they work within the industry to become fully compliant.

The Commission requires voice service providers to develop a Robocall Mitigation Plan that:

- details the reasonable steps taken to avoid originating illegal robocalls
- demonstrates a commitment to respond to traceback requests to cooperate with investigating and stopping illegal robocalls
- is filed in the Robocall Mitigation Database

ComTec Cloud Services LLC (ComTec) is a business voice service provider that provides voice and contact center solutions to business through the use of SIP based services throughout the US. ComTec is partnered with other trusted Service Providers who have implemented STIR/SHAKEN and will continue to work with the rest of our partners to ensure all aspects of our delivery comply with the appropriate requirements.

ComTec is categorized by the FCC as a small service provider with less than 100,000 subscriber lines. Currently the FCC has extended the deadline of June 30, 2021 to June 30, 2023 for small service providers to implement STIR/SHAKEN and has since on April 29, 2020 proposed to shorten that extension deadline to June 30, 2022. While ComTec works on its plan to become compliant with STIR/SHAKEN within the current 2023 deadline, we will stay abreast of the FCC Call Authentication Trust Anchor WC Docket No 17-97 decision and adjust our timeline accordingly, if need be.

This plan outlined is provided by ComTec is to provide additional details on how ComTec will provide mitigation and investigation efforts from its platforms.

Limiting Originating Traffic:

ComTec provides Individual Hosted PBX and/or SIP trunks to client PBXs. Within our hosted service, we require authentication for devices to be able to utilize the PBX and place calls outside of the PBX. This authentication limits the ability for an outside party to conduct any

robocalling through our services unless originating from a client not within our control. With our SIP trunks and our hosted PBXs we limit what can be sent out to our SIP providers and only originate numbers that have been ported to our platforms. This additional step helps limit the ability for someone to perform Robocall services through our platform.

Proactive Monitoring:

Utilizing platforms purchased from known vendors in the SIP industry, we collect information from all calls traversing our services provided through our Datacenters. This information is used for quality and CDR purposes. Through the process of collecting this information we can provide origination and termination details including SIP headers to allow proper personnel to understand where the call came from and its intended destination.

Alarms:

By utilizing our proactive monitoring platform we have enabled many different types of alarms that trigger without human interaction and receive notification via several different methods including but not limited to Emails, tickets, and texts. Some of these alarms are listed below.

Triggers:

- # of calls within a specified period of time
- Long duration calls
- Calling Loops
- Sequential # calling

Investigations:

Any and all investigations of calls within our platform are performed within our engineering teams and will be tracked and documented within our ticketing system. This allows for timely investigation with documented steps and results. We require official requests from any party that is looking to gain additional details of calls originating from within or through our platforms.

Call Blocking:

ComTec has documented procedures on how to block certain calling or called numbers to assist with a span of reasons for needing to block calls. This can range from illegal or suspected illegal calls, spam calls, or fraudulent calls. Any of our engineers can perform this action to allow for timely resolution of requests made by clients, or members of prevailing authority when requested.