

SIPtech PBX Robocall Mitigation Policy

Robocall Mitigation Compliance with TRACED Act

Date	On behalf of	Change Summary
May 24, 2024	SIPtech PBX	Version 1.0

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

I. 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.

This mitigation plan is submitted on behalf of SIPtech PBX, an IP telephony and technology company, and its wholly owned subsidiary, RT2 Tech., a provider of competitive local SIP services. SIPtech PBX serves the Houston metro area in the state of Texas. Both companies share operations, including their respective Robocall Mitigation Plans and will be referred to as SIPtech throughout this document.

SIPtech is a small voice service provider offering SIP services primarily in the greater Houston area.

SIPtech utilizes SIP trunk services provided by Skyetel and have setup STIR/SHAKEN protocol as directed by Skyetel provider.

II. General Prohibition Against Illegal Robocalling

SIPtech end user services are subject to restrictions contained in its published legal notices and all executed services orders include the requirement that service is provided pursuant to its terms of service (“TOS”) requirements.

Its existing TOS prohibit 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;

Robocall Mitigation Policy

- violating any applicable local, state, or federal law; using the SIPtech service to engage in or in connection with fraudulent activities.

In addition, the company is updating its TOS to expressly reference the prohibition on robocalling and all current subscribers will receive notice of the publication of its updated TOS.

SIPtech's end users are notified that SIPtech may take action up to suspension or termination of service for violation of the TOS.

III. Know Your Customer

SIPtech utilizes the mitigation technique of “Know Your Customer.” SIPtech is a small long established provider that maintains a close relationship with its subscribers. Its customers are generally “mom and pop” users and few of its total customer base have enough call paths to generate the high volume of traffic associated with robocalling allowing us to use targeted in-house analytics to monitor, alert and apprehend suspected robocalling activities.

SIPtech has set a call path level based on its average customer size. The level – referred to as “large volume calling capability” – is subject to change.

SIPtech has a screening for new customers requesting service at or above large volume calling capability levels:

- We will not deploy large volume calling capability as a residential service or at an address shown in the company records as being residential
- Businesses requesting large volume calling capability must provide a tax ID and verification as to the nature of the business
- We verify addresses to look for overlapping / multiple deployed voice path subscriptions
- A SIPtech representative may visit the premise of the business to verify the number of users at the location is appropriate for the volume of calling

SIPtech serves a small number of long-time business end users with small volume calling capability and have limits placed on number of minutes for outgoing calls. SIPtech also utilizes alerts to detect any abnormal behaviour.

IV. Network Monitoring

SIPtech has both network monitoring alerts configured for traffic increases or daily monetary spend which will alert management of abnormal or increase usage. We have the ability to immediately take corrective action against these alerts.

Robocall Mitigation Policy

V. Traceback and Enforcement Cooperation

SIPtech will actively cooperate with the traceback community including the FCC, law enforcement, and The Industry Traceback Group (ITG) to investigate and stop illegal robocalls. SIPtech will dedicate sufficient resources to provide prompt and complete responses to traceback requests.