

# Robocall Mitigation Policy

---

## Robocall Mitigation Compliance with TRACED Act

| Date        | On behalf of | Change Summary  |
|-------------|--------------|-----------------|
| Jan 9, 2021 | Nimbus       | Initial Version |

---

|                   |                                                                 |
|-------------------|-----------------------------------------------------------------|
| <b>Objective:</b> | 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 Nimbus, a voice platform. Nimbus provides a voice platform for companies to manage their call centers.

Nimbus is partnering with our underline carriers to implement STIR/SHAKEN in parts of its network.

### II. General Prohibition Against Illegal Robocalling

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

# Robocall Mitigation Policy

---

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.

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

## **III. Know Your Customer**

Nimbus utilizes the mitigation technique of "Know Your Customer." Its customers are generally small to medium business users. Generally these customers can vary with all different volumes of calling. In order to combat abuse we have implemented the following:

- We do a video conference with the customer to verify their identity.
- During our video call we question their current traffic, their compliance practices, etc.
- All Businesses 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 Nimbus representative may, if local, visit the premise of the business to verify the number of users at the location is appropriate for the volume of calling

## **IV. Network Monitoring**

Nimbus is continuing development of custom software in-house that allows for real-time monitoring of traffic and will flag call patterns indicative of potential illegal robocalling. Additionally we listen to any complaints received from our providing carriers. If a complaint is received we typically will begin asking the customer for all compliance documentation on the person that complained to see if any violation occurred.

## **V. Traceback and Enforcement Cooperation**

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