

Robocall Mitigation Policy 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 Central Park Systems DBA Fortis (Fortis).

Fortis is a small voice service provider with SIP services in its network and we believe we are temporarily exempt from the requirements of §64.6301 as we participate with the industry to find an implementation solution before June 30, 2023.

Fortis is partnering with a trusted provider to implement STIR/SHAKEN in parts of its network as it is realistically able to do so and has implemented this policy for those portions of its network not yet compliant.

II. General Prohibition Against Illegal Robocalling

Fortis services are subject to restrictions contained in its published Acceptable Use Policy (AUP) and all executed services orders include the requirement that service is provided pursuant the terms of the AUP.

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 Fortis 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.

Fortis' customers are notified that Fortis may take action up to suspension or termination of service for violation of the AUP.

Robocall Mitigation Policy III. Know Your Customer

Fortis utilizes the mitigation technique of "Know Your Customer." Fortis is a small, regional provider that maintains a close relationship with its subscribers. Its customers are generally small, local businesses 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.

Fortis set a call path level based for each customer which caps the overall call paths and the outbound call paths. The call path level is set based on the number of endpoints.

Fortis has a screening procedure 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
- A Fortis representative may 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

Fortis is currently evaluating technology partners to allow for real-time monitoring of traffic and will flag call patterns indicative of potential illegal robocalling. Additional capability may include software which will automatically disable any subscribers associated with flagged call patterns.

V. Traceback and Enforcement Cooperation

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

VI. Revision History

Date	Change	Revision
6/01/2020	Initial Release	1.0
12/3/2024	Revised	2.0