

Robocall Mitigation Policy

Robocall Mitigation Compliance with TRACED Act

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 Whooster, Inc. Whooster provides investigative data to government and enterprise customers through a variety of electronic methods. One of those methods is SMS/MMS Text Messaging. Whooster partners with a number of SMS gateway companies to provide this data, which makes Whooster a reseller of telecommunications services. Whooster has been advised that it must register in the RMD because of this reseller status. Whooster does NOT provide voice origination or termination services to end users. Whooster is filing this mitigation plan as required for a traditional voice reseller, but does not anticipate that any customer or robocall activity will ever take place using any Whooster services.

II. General Prohibition Against Illegal Robocalling

Whooster 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 Whooster service to engage in or in connection with fraudulent activities

Whooster end users are notified that Whooster may take action up to suspend or terminate service for violation of the TOS.

III. Know Your Customer

Whooster utilizes the mitigation technique of “Know Your Customer.” Whooster is a long established provider that maintains a close relationship with its subscribers. Its customers are generally governmental agencies or Fortune 500 enterprise companies. These customers use Whooster for data and software analytics. They do not have access to Whooster’s voice network and are not the type of clients who engage in robocalling.

IV. Network Monitoring

Whooster is continuing development of custom software in-house that allows for real-time monitoring of all kinds of traffic, including data, SMS and Voice. Whooster will flag call patterns indicative of potential illegal robocalling. Whooster’s voice termination partners also have robocalling pattern matching and will also notify Whooster of any suspicious traffic that crosses their networks.

V. Traceback and Enforcement Cooperation

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