



ROBOCALL Mitigation Plan and Protocol

FRN: 0033592122

Last updated: 4/10/2023

Effective: 4/1/2023

I. **Overview**

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

The Commission requires voice service providers (VSP) to develop a RMP that:

- A. Details the reasonable steps taken to avoid originating illegal robocalls
- B. Demonstrates a commitment to respond to traceback requests to cooperate with investigating and stopping illegal robocalls
- C. Is filed in the RMD

This mitigation plan is submitted on behalf of Over The Top Marketing Corporation (OTT), a voice service provider. OTT services small businesses (largely locations owned by franchisees of brands in the health, wellness, and beauty industries).

OTT partners with trusted providers to implement STIR/SHAKEN in all of its networks.

II. **General Prohibition Against Illegal Robocalling**

OTT end users are subject to technical and contractual limitations to prevent 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 local, state, or federal law; otherwise using OTT services in connection with any fraudulent activities.

III. **Know Your Customer & Technical Limitations**

OTT utilizes a mitigation technique of "Know Your Customer." OTT maintains a close relationship with each of our clients and the Brands that they are part of. Generally, each of these clients are small businesses without sufficient customers that could be reached by a high enough volume of call traffic associated with robocalling making it easier to monitor the overall traffic for spikes in traffic indicative of robocalling activity.

Technical limitations are in place as well. Customers do not have direct access to SIP

endpoints nor have the ability to perform any outbound calls over our network without utilizing software built into OTT's password-protected systems (Carbon and Advantage). The technology provided to our clients limits activity to one-to-one communications.

IV. **Network Monitoring**

OTT keeps track of all outbound calls generated over its networks and monitors it for any activity indicative of Robocalling. OTT has an alert set to proactively notify our Network Operations team of suspiciously high volume of calls originating from any of the numbers that we provide to our clients.

V. **Traceback and Enforcement Cooperation**

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