

Robocall Mitigation Policy

Robocall Mitigation Compliance 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 Shift Computer Services, a VOIP service provider.

II. General Prohibition Against Illegal Robocalling

Shift Computer Services 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 prohibits 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 Shift Computer Services service to engage in or in connection with fraudulent activities

III. Know Your Customer

Shift Computer Services utilizes the mitigation technique of “Know Your Customer.” Shift Computer Services is a small, long established provider that maintains a close relationship with its subscribers. Its customers are generally small businesses, and none are using automated “Robocalling” systems. All customers by default are limited to reasonable call concurrency sufficient to perform their daily activities without the possibility of mass outbound call campaigns.

Robocall Mitigation Policy

IV. Network Monitoring

Shift Computer Services employs a system that allows for real-time monitoring of traffic and will flag call patterns indicative of potential illegal robocalling. Any account violating the TOS will be disabled pending an investigation.

V. Traceback and Enforcement Cooperation

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