

MCSP, INC. ROBOCALL MITIGATION PROGRAM

Below is the Robocall Mitigation Plan filing for MCSP, Inc. This plan will be submitted to the FCC's Robocall Mitigation Database and will be adapted to adjust to the latest laws, regulations, and industry best practices.

Monitoring

MCSP, Inc. has monitoring and reporting systems in place to analyze high-volume voice network traffic to identify and monitor patterns consistent with robocalls. Our monitoring systems provide alerts on calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated Telephone Number (TN) to detect patterns consistent with illegal robocalls.

If MCSP, Inc. detects a pattern consistent with illegal robocalls, or we have reason to suspect illegal robocalling or spoofing is taking place over our network, we will seek to identify the party that is using our network to originate, route, or terminate these calls. and take appropriate action.

Appropriate action may include:

- Validating that the originating party is authorized to use the TN.
- Suspending calling party's ability to originate, route, or terminate calls on MCSP, Inc. network.

Traceback Cooperation

MCSP, Inc. commits to responding in a timely manner and supporting all traceback requests from the FCC, law enforcement, and the [Industry Traceback Group \(ITG\)](#).

Bulk Solutions Robocall Mitigation Solution Overview

- General information
 - Robocall scoring is based on the annual +100B carrier calls that Bulk Solutions processes as part of the Caller Name service.
 - STIR/SHAKEN Transaction Detail Records (TDRs) are now being added as an additional data source.
 - Each call is assessed through the Bulk Solutions model, leading to constantly refreshed view of call behavior and probability of a given number currently being used for robocalling.
 - Active numbers are assessed by the model for behavioral attributes typically associated with robocalling including:
 - Neighbor spoofing events
 - Sudden spikes in volume, such as driven by call spoofing
 - Do-Not-Originate (DNO) numbers are also deemed to be robocalls if they are the calling party number. This is sourced from industry (e.g., US Telecom) and directly from enterprises.
 - The service covers both US domestic and international TNs.

- Calls originating from your network (i.e., Robocall Protection)
 - Provides detailed reporting identifying suspected illegal robocalls and alerts if calls originate where the calling number is invalid, unallocated, on a Do-Not-Originate list.
 - If the platform detects a suspected robocalling patterns MCSP, Inc. will take appropriate action which may include suspending or terminating the subscriber.
 - Supports a real time query to service to determine if a number originating on your network could be a robocall. Such calls can be blocked, or the terminating party can be notified via CNAM.
 - For each new instance of robocalling using the Operating Service Provider (OSP)TNs, an alert is sent to the OSP in near real time. This alert will result in the OSP (manually) blocking the TN and all TSPs being alerted via CNAM, through an overlay such as “ROBOCALLER”. The CNAM alerting helps address instances of spoofing of TNs that are not going through the OSP that owns the number.

- Termination (i.e., Robocall Mitigation)
 - Supports a real-time query to service to determine if a number terminating on your network could be a robocall. This protects subscribers from calls that come from networks that cannot authoritatively attest to the end user caller (i.e., all Communications Service Providers (CSPs)that do not have STIR/SHAKEN and all CSPs *with*STIR/SHAKEN, but who do not have a direct and vetted end user relationship.)
 - Such calls can be blocked or the called party can be notified via CNAM.

Call48 Robocall Mitigation Plan

Purpose

Call48 is dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network consistent with Federal Communications Commission (“FCC”) regulations.

Call48 has implemented the STIR/SHAKEN call authentication protocol in the IP portions of its network. STIR/SHAKEN does not, however, cover the TDM portions of Call48’s network. Therefore, Call48 has also adopted the policies and procedures set forth in this document to comply with the FCC’s anti-Robocalling regulations. This document defines Call48’s Robocall Mitigation plan.

“Know Your Customer” (“KYC”)

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with Call48 through which we transit, originate and/or terminate calls on behalf of the subscriber.

Call48’s KYC program requires a signed contract with our subscriber. Prior to signing a contract, Call48 confirms a subscriber’s identity by vetting a subscriber directly or by using a third-party vetting service. The vetting process includes collecting information such as:

- physical business location,
- contact person(s),
- state or country of incorporation,
- federal tax ID,
- nature of the customer’s business.

Telephone Number Authorization

For the purposes of this plan, a Telephone Number (TN)-based caller identity is defined as the originating phone number included in call signaling used to identify the caller for call screening purposes that is uniquely associated with a subscriber. A TN used for caller identity may or may not be associated with the subscriber’s account with the responsible party.

A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by Call48 and/or obtained by Call48 from one of Call48’s underlying carriers for use by the subscriber. In most cases, Call48 directly manages TNs used by its subscribers. Call48 tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Call48’s assignment of the TN to its subscriber.

When originating a call, Call48 checks the calling party number (also called the ANI) against Call48’s inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

Monitoring

Call48 has monitoring and reporting systems in place to analyze high-volume voice network traffic to identify and monitor patterns consistent with Robocalls. Our monitoring systems alert on calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated ANIs to detect patterns consistent with illegal Robocalls and attempts at illegal call spoofing.

If Call48 detects a pattern consistent with illegal Robocalls, or we have reason to suspect illegal

Robocalling or spoofing is taking place over our network, we will seek to identify the party that is using our network to originate, route, or terminate these calls and take appropriate action.

Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating commercial customer owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate, route, or terminate calls on our network.

Investigation of Suspicious Activity and Traceback

Call48 follows USTelecom Industry Traceback Group ("ITG") recommended industry best practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Call48 will dedicate sufficient resources to provide prompt and complete responses to traceback requests.

Call48 will investigate suspicious activity found by its monitoring systems or reported to Call48 by consumers or third parties. The investigation could potentially result in opening a traceback request or with Call48 contacting a subscriber to correct improper use of the platform, or, if the subscriber or subscriber's End-User does not respond or comply, to block their use of the platform.

For all new and renegotiated Call48 contracts governing the transport of voice calls, Call48 intends to contractually require Call48's subscribers to cooperate with in traceback investigations by identifying the upstream provider from which the suspected illegal Robocall entered our network.

Blocking

When it is administratively feasible, Call48 will implement Do Not Originate ("DNO") requests it receives from the ITG.

If Call48's monitoring systems identify suspected Robocalling patterns that are confirmed with further investigation, Call48 will take appropriate action which may include suspending or terminating the subscriber's or End-User's use of Call48's network.

Plan Updates

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal Robocalling. Call48 will monitor industry best practices and continuously improve our internal processes to ensure this plan and our systems adapt to this ever-changing issue.