

Telesupply, LLC
Robocall Mitigation Plan

Introduction

This document details the reasonable steps and actions taken by Telesupply, LLC (“Telesupply”) to mitigate and eliminate illegal robocalling. Telesupply has an ongoing commitment to scan for and help alleviate illegal robocalling by pre-qualifying prospective customers, monitoring existing customers for traffic patterns indicative of prohibited robocalls, and working with other providers and regulatory agencies in combatting fraudulent voice activity.

Telesupply provides interconnected Voice over Internet Protocol (“VoIP”) calling services. Telesupply has fully implemented the STIR/SHAKEN authentication framework across our entire network, and all calls we originate are compliant with § 64.6301(a)(1) and (2). Telesupply has our own token and OCN 236L.

Know Your Underlying Provider

Telesupply, LLC has a master service agreement with our upstream provider, Sangoma. Through Telesupply’s Terms and Conditions, we mandate that each agreement with our upstream providers incorporates strict policies pertaining to fraudulent calls. Our upstream providers agree to abide by the FCC’s STIR/SHAKEN and robocall mitigation rules in all respects when providing voice services. Telesupply and its provider partners have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Know Your Customer

Screening interviews are performed to understand potential customer business models and the potential, or lack thereof, for involvement in fraudulent robocalling schemes. Telesupply performs due diligence on all business customers prior to service activation. This includes collecting company formation documents, physical address verification, business license, EIN, and the name(s) and contact information of responsible parties. We verify incorporation status via Secretary of State databases and require payment via a valid U.S. business bank account. We do not activate accounts with anonymous or unverifiable ownership.

In our research of the prospect, Telesupply will not activate clients that provide anonymous information or where data mismatches are found. Additionally, prospects are required to agree to Telesupply’s strict policies and contractual terms prohibiting the act of fraudulent voice activity as a condition of doing business with Telesupply.

Individuals associated with prospects or current customers who have been known to act improperly or otherwise be involved in fraudulent robocalling will cause their companies to be rejected by Telesupply as a customer and any existing customer relationships could potentially be severed.

Traceback Requests

Telesupply is committed and will respond fully within 24 hours to all Traceback Requests from the FCC, law enforcement agencies, and the industry traceback consortium and vows to cooperate with these agencies in investigating and stopping any illegal robocallers that use our service to make calls. Telesupply will devote sufficient resources to provide prompt and complete information to traceback requests. Our points of contact to handle all traceback requests are:

Richard Valle Jr

CEO

562-333-3131

rvalle@telesupply.com

Alex Hurt

Tier 3 Support Manager

phonesupport@telesupply.com

Telesupply provides VoIP services to business customers and implements a multi-layered robocall mitigation program. All customers undergo identity verification including EIN verification, business registration checks, and usage reviews before service activation. We maintain call records, monitor for high-risk traffic patterns, and cooperate fully with traceback requests. We do not offer service to high-risk call centers or international originators using NANP numbers. Telesupply uses sangoma.com as its upstream PSTN carrier, which performs STIR/SHAKEN signing on our outbound calls.

If a traceback exposes an existing customer as the source of fraudulent robocalls, or as having transmitted fraudulent robocalls, a demand for an explanation and verification of mitigation of the traffic is issued to the customer. If the fraudulent traffic is not remediated, Telesupply immediately begins rejecting all traffic from the offending customer.

Telephone Numbers

A Telephone Number (“TN”) based caller identity is the originating phone number included in call signaling used to identify the caller for screening purposes that is uniquely associated with the subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by Telesupply and/or obtained by Telesupply from Telesupply’s underlying carrier for use by the subscriber. Numbers can also be ported using information from previous bill matching customer information.

Telesupply verifies each customer’s right to use assigned telephone numbers through its provisioning systems and number porting process. Numbers are only assigned to validated customers and are tied to an account with documented KYC details. We do not currently use a third-party number validation service, but we monitor all number usage patterns for anomalies and take corrective action if misuse is suspected.

International Calling

Telesupply is not currently an international voice services provider. If at any time Telesupply does decide to sell our services to international customers using North American Numbering Plan resources, we will familiarize ourselves with and develop best practices for full vetting of such customers and work with our underlying provider to perform the necessary telephone number validation on all international originated calls.

Call Analytics

Telesupply uses internal monitoring tools and CDR (Call Detail Record) analysis to identify abnormal calling patterns, such as high volumes of short-duration calls, repeated call attempts to invalid numbers, or sudden traffic spikes. Our upstream provider, Sangoma, applies STIR/SHAKEN and additional robocall analytics on all outbound calls traversing their network. While Telesupply does not currently use a third-party analytics vendor directly, we rely on Sangoma's analytics stack for call validation, fraud detection, and network-level blocking of suspected illegal robocall traffic.

Ongoing Robocall Mitigation

If illegal or suspicious traffic is detected, Telesupply investigates immediately by analyzing call records and usage patterns. Our terms of service allow for suspension or termination of accounts found to be in violation of robocall policies. We act quickly to mitigate traffic, notify upstream carriers, and cooperate with traceback requests. Customer contracts explicitly prohibit illegal robocall activity. We also have direct contact with the end user to terminate all outbound call activity during mitigation.

Telesupply does not accept traffic from unknown or unauthenticated third-party sources. All inbound and outbound traffic flows through our managed services infrastructure via Sangoma. As an Originating Service Provider, we only enable outbound calling for verified end users. We do not act as an intermediate provider and do not accept wholesale traffic. Therefore, blocking unregistered voice providers is inherently managed by our closed customer model and reliance on Sangoma, who monitors Robocall Mitigation Database compliance at the network level.

Telesupply Contact for Robocall Mitigation-Related Issues

The Company will update our Robocall Mitigation filings within 10 business days of any change to the information outlined in this plan. Please direct any questions related to Robocall Mitigation issues to:

Richard Valle Jr, CEO
4332 Cerritos Ave suite 108
Los Alamitos CA 90720
562-333-3131
rvalle@telesupply.com