

Robocall Mitigation Plan

Company: Tele-SyS, Inc.

Contact: Curtis Jamison

FRN: 0003770120

OCN: 5633, 7652

Address: 673 Emory Valley Road, Oak Ridge, TN 37830

Telephone: 865-482-2140

Email: jamisoncs@accessam.com

Date: April 26, 2024

Summary

Tele-SyS is a small reseller providing POTS and TDM services to the majority of customers and VoIP services to a small portion of customers in niche situations. We have been in business since 1982. Our customer base consists of small business and a few residential customers. We are committed to preventing originating illegal robocall traffic and to block calls associated with illegal robocalling activity. This document certifies our partial implementation of the STIR/SHAKEN standards, in compliance with FCC guidelines.

Our customers are known to us

Since 1982, we have provided telephone services to small businesses and residential customers. Our customers are known to us. We obtain information regarding their identity, location and we verify their identities and often meet with them face-to-face as part of the service initiation process. All of our services are post-paid services and we do not provide pre-paid or cellular or other wireless services. The information we obtain prior to establishing service for a customer includes legal business name, federal tax identification number and physical address for installation of phone services and is used to verify the identity of the business or residential subscriber. We ask questions of the customer to determine their usage of the service and do not currently, nor do we anticipate providing service to call centers or other customers that would intend to engage in robocalling services.

Customers are prohibited from abusive, fraudulent or unlawful use of any service

All customers are prohibited from abusive, fraudulent, or unlawful use of any service. Any use of the service for abusive, fraudulent, or unlawful means is subject to termination of services.

Identifying fraudulent call patterns

For TDM services, which are the majority of our services, we rely on in-house analysis of call patterns and on our underlying carriers to alert us to fraudulent call patterns and will work with our underlying carriers to identify those patterns and sources of fraudulent calls if and when they occur. The types of information that we would analyze to indicate fraudulent calls include average call duration, call completion rates, calling identification name and number, call volumes and the timeframes in which calls are placed, sequential dialing patterns, apparent location of the caller, and calls to areas known to be high risk for fraudulent traffic or illegal robocall schemes. If a fraudulent pattern is detected, the customer is contacted to determine if the customer is engaged in fraudulent calls, illegal robocalling or spoofing. For VoIP services, which are a small minority of our services, we rely on our underlying carrier of the hosted phone (hosted PBX) systems to maintain robocall prevention and will work with the underlying carrier to identify and terminate service if and when robocalls occur. If the customer is engaged in fraudulent calling, illegal robocalling or spoofing, the service to the customer can be terminated or restricted until the fraudulent, illegal robocalling or spoofing patterns are resolved.

Traceback requests

We will cooperate with traceback requests and subpoenas from the FCC and law enforcement and cooperate with those requests in investigating and stopping any fraudulent or illegal activities, including illegal robocall activity.