

Robocall Mitigation Program for VoIP.ms Reseller (No STIR/SHAKEN Obligation)

This document outlines a Robocall Mitigation Program for a VoIP.ms reseller who does not have a direct obligation to implement STIR/SHAKEN. This program is designed to comply with FCC regulations requiring all voice service providers to take reasonable steps to mitigate robocalls.

I. Introduction

St. Charles Consultants d/b/a St. Charles IT Consultants is committed to preventing the origination and transmission of illegal robocalls. While we operate as a reseller of VoIP.ms services and may not have direct control over the underlying network infrastructure for STIR/SHAKEN implementation, we recognize our responsibility to take proactive measures to mitigate robocall traffic. This program details the steps we take to fulfill this responsibility.

II. Program Components

Our Robocall Mitigation Program consists of the following key components:

- **A. Know Your Customer (KYC) Procedures:**

- We implement thorough KYC procedures for all new customers to verify their identity and legitimacy. This includes:
 - Collecting and verifying business registration information (if applicable).
 - Obtaining and verifying the customer's physical address.
 - Requiring detailed information about the customer's intended use of VoIP services, including the types of calls they will be making and how they obtain consent (if required).
 - Checking for any red flags, such as suspicious business activity or a history of complaints.
 - For high-volume customers, we may request additional documentation, such as references or financial statements.
- We maintain accurate and up-to-date customer records.

- **B. Monitoring and Analysis:**

- We monitor customer calling patterns and traffic for suspicious activity. This includes:
 - Analyzing call detail records (CDRs) for patterns indicative of robocalls, such as:
 - High call volumes in short periods.
 - Short-duration calls.
 - A high number of abandoned calls.

- Unusual calling times.
 - Tracking customer complaints and reports of unwanted calls.
 - Using available tools and reports from our underlying provider (VoIP.ms) to identify potential robocall activity.
- **C. Enforcement and Remediation:**
 - We have established procedures for investigating and addressing suspected robocall activity. This includes:
 - Contacting customers to inquire about suspicious calling patterns.
 - Issuing warnings to customers who violate our robocall mitigation policies.
 - Suspending or terminating service for customers who engage in illegal robocall activity.
 - Cooperating with law enforcement and industry traceback efforts to identify and stop robocallers.
- **D. Coordination with VoIP.ms:**
 - We maintain close communication with VoIP.ms to stay informed about their robocall mitigation efforts and to coordinate our activities. This includes:
 - Understanding VoIP.ms's STIR/SHAKEN implementation status and their other robocall mitigation measures.
 - Reporting any identified suspicious activity to VoIP.ms.
 - Cooperating with VoIP.ms in any investigations of robocall traffic.
 - Ensuring our policies and procedures are consistent with VoIP.ms's requirements.
- **E. Policy Updates and Review:**
 - We regularly review and update our Robocall Mitigation Program to ensure its effectiveness and compliance with evolving regulations and industry best practices. This includes:
 - Monitoring FCC regulations and industry developments related to robocalls.
 - Reviewing our program at least annually.
 - Making necessary adjustments to our policies and procedures.
- **F. Robocall Mitigation Database Filing:**
 - We will file this Robocall Mitigation Program with the FCC Robocall Mitigation Database, as required. We will keep our filing accurate and up-to-date.

III. Specific Reasonable Steps

In accordance with FCC requirements, St. Charles Consultants d/b/a St. Charles IT Consultants is taking the following specific reasonable steps to avoid originating or transmitting illegal robocall traffic:

1. **Customer Vetting:** We employ a detailed KYC process (as described in II.A) to verify customer identity and intended use of services. This is our first line of defense.
2. **Traffic Analysis:** We actively monitor call traffic for patterns indicative of robocalls (as described in II.B).
3. **Prompt Action:** We commit to taking swift action when we identify suspicious activity, including customer contact, warnings, suspension, or termination of service (as detailed in II.C).
4. **Provider Collaboration:** We work closely with VoIP.ms, our upstream provider, to enhance robocall mitigation efforts. This includes providing them with information and cooperating with investigations (as described in II.D).
5. **Compliance:** We stay current with FCC regulations and update our program as needed (as described in II.E).
6. **Database Filing:** We will file and keep our robocall mitigation plan updated in the FCC Robocall Mitigation Database.

IV. Responsibilities

The following individuals/departments are responsible for implementing and overseeing this Robocall Mitigation Program:

- Chris Weindel/Telecommunications Services Operations: Responsible for KYC procedures and customer onboarding.
- Chris Weindel/Telecommunications Services Operations: Responsible for monitoring call traffic and analyzing CDRs.
- Chris Weindel/Telecommunications Services Operations: Responsible for investigating and taking action on suspected robocall activity.
- Chris Weindel/Telecommunications Services Operations: Responsible for compliance with FCC regulations and program updates.
- Chris Weindel/Telecommunications Services Operations: Responsible for Robocall Mitigation Database Filings

V. Record Keeping

We maintain records related to our Robocall Mitigation Program, including:

- Customer KYC documentation.

- Call monitoring data and analysis reports.
- Records of actions taken in response to suspected robocall activity.
- Records of communication with VoIP.ms regarding robocall mitigation.
- Copies of our Robocall Mitigation Program and any updates.
- Proof of filing with the FCC Robocall Mitigation Database.

VI. Conclusion

St. Charles Consultants d/b/a St. Charles IT Consultants is dedicated to preventing the misuse of our services for illegal robocalls. This Robocall Mitigation Program outlines the steps we take to achieve this goal. We believe that these measures are reasonable and appropriate for a VoIP.ms reseller, and we are committed to ongoing improvement and adaptation to combat the evolving threat of robocalls.