

CSS Infotech

Robocall Mitigation Plan

Robocall Mitigation Program Overview

Css Infotech, based in India, is a global technology service provider and International Technology Service Provider (ITSP), offering international communication services. We purchase voice minutes from global providers and resell them to our clients. In doing so, Css Infotech strictly adheres to the rules, regulations, and orders of the Federal Communications Commission (FCC), particularly concerning short-duration traffic and other telecommunication guidelines.

Pursuant to 47 C.F.R. § 64.6305, we hereby submit this report on our implementation of the STIR/SHAKEN framework and outline the measures taken to prevent and mitigate illegal robocalls. This document details the current status of our STIR/SHAKEN integration and describes the proactive strategies we have in place to combat illegal robocalling.

We may adjust or amend these policies and procedures in response to evolving business needs, regulatory requirements, or operational capabilities.

Measures Taken to Prevent Illegal Robocalls Originating from Our Platform

1. Customer Documentation

At onboarding, we verify customer identities by collecting valid proof of identity and address. We also establish specific agreements with customers that clearly outline the acceptable usage of our platform.

2. Robocall Detection and Mitigation

We employ advanced data analytics to identify illegal robocall patterns, such as short, high-frequency calling bursts or uniform call lengths. In cases where suspicious activity is detected—such as high-volume traffic directed to a specific destination using a single or multiple caller IDs (CLI)—we collaborate with the relevant carriers to verify the authenticity of the calls. If needed, we block partial traffic and escalate for resolution.

3. Industry Collaboration

Css Infotech cooperates fully with industry traceback efforts and responds promptly to law enforcement requests. We enforce strict CLI (Caller Line Identification) management, allowing only authorized CLIs that are obtained through verified channels. If a customer wishes to use their own CLI, they must undergo a Call OTP (One-Time Password) authentication process to validate their CLI via an active number.

4. STIR/SHAKEN Implementation

Our network is capable of passing STIR/SHAKEN tokens as they are received, and we maintain the certification level granted to us without modification. Additionally, we have enforced network-wide restrictions designed to mitigate short-duration traffic. These include an ANI (Automatic Number Identification) Blacklist, which blocks calls from flagged ANIs, as well as blocking any calls to numbers on the Do Not Call (DNC) list.

Customer Due Diligence and Obligations

Onboarding Procedures

The VoIP platform we use for call switching enables us to enforce rigorous compliance standards for clients, ensuring adherence to international telecommunications regulations.

1. Spam Filtering

- **In-House Spam Filter:** We use an internal spam filtering solution, which continuously evolves to block spam and scam calls.
- **IPQS Spam Filter:** A premium third-party spam filtering service ensures comprehensive protection against unwanted or malicious calls.

2. KYC (Know Your Customer) Compliance

We partner with Stripe and other KYC platforms to verify customer identities, including cross-checking company registration details to ensure authenticity.

3. Real-Time Call Analysis

We use real-time call transcription analysis (Class 4) to detect robocall campaigns and other potentially fraudulent activity. This process occurs without recording audio, thus maintaining customer privacy. If flagged, customers must consent to call recording for further fraud analysis.

4. Customer Education and Responsibilities

- **Telecom Security Education:** Customers receive training on telecom safety and fair usage policies.
- **Compliance Agreement:** Each customer must sign an agreement acknowledging their understanding of telecom security and agreeing to abide by their responsibilities. Failure to comply may result in account suspension and notification to authorities.
- **Fraud Detection:** Customers flagged for suspicious activity must consent to call recording and analysis. Verified instances of fraud will be reported to relevant authorities, with detailed documentation of the violations.

Ongoing Monitoring and Enforcement

1. Automated Monitoring Systems

- **Spam Filters:** Our spam filters operate continuously, leveraging an evolving algorithm to block spam calls in real time.
- **Real-Time Call Analysis:** The system continuously analyzes call traffic, flagging any suspicious behavior without recording the audio. Alerts are sent to management if pre-set thresholds are breached, prompting a decision on whether to issue warnings or take other corrective measures.

2. Manual Checks and Periodic Reviews

- **KYC Reverification:** We periodically update and review KYC documentation to ensure ongoing compliance.
- **Manual Investigation:** If a customer is flagged for suspicious activity, we conduct a thorough manual investigation. Customers must consent to having their calls recorded for analysis. Any confirmed cases of regulatory non-compliance are escalated and addressed appropriately.

3. Automated Actions on Breach

If a customer violates spam or scam policies, the system may automatically initiate the following actions:

- **Traffic Suspension:** Temporary suspension of traffic.
 - **Account Suspension:** Temporary suspension of the customer's account.
 - **Show Cause Notice:** Issuance of a formal investigation or warning notice.
-

Response to Traceback Requests and Collaboration

Css Infotech remains committed to full cooperation with traceback requests from the FCC, law enforcement, and the registered traceback consortium. Upon receiving a traceback request, we will investigate within 48 hours, providing any available data for the specified calls. Additionally, we plan to integrate our systems with the Industry Traceback Group (ITG) to further expedite the traceback process.

We leverage internal software to monitor outbound traffic in real-time, ensuring the detection and prevention of illegal robocalls. This software generates detailed reports, identifies suspicious calls, and flags any calling numbers that appear invalid, unallocated, or listed in the FCC complaint database. If any calls are deemed unlawful, we take immediate action, which may include issuing warnings, blocking calls, or terminating service as per industry standards.

For further information or assistance, please feel free to contact us at: **compliance@cssinfotech.in**

We remain dedicated to working in collaboration with regulatory authorities and law enforcement agencies to safeguard the integrity of telecommunications and protect consumers from fraudulent activities.