

Robocall Mitigation Plan

TECHNOLOGY CABLING INC.

1. Introduction

TECHNOLOGY CABLING INC. (“TECHNOLOGY CABLING”) is a voice service provider that offers direct IP-based telephony services to end users using SIP technologies. Our primary customer base consists of residential users, with a limited number of commercial accounts restricted to research-related use cases. We do not support or provide services for automated dialer applications.

Given our residential focus, fixed caller-ID assignment, and per-account call limits, TECHNOLOGY CABLING assesses its exposure to illegal robocall activity as low-to-moderate. Nonetheless, we maintain robust mitigation measures to detect, prevent, and respond to any misuse of our network.

2. Technical Safeguards

TECHNOLOGY CABLING deploys multiple technical controls to prevent, detect, and remediate robocall and other fraudulent traffic.

2.1 STIR/SHAKEN Implementation

TECHNOLOGY CABLING has fully implemented the STIR/SHAKEN caller-ID authentication framework across its network. All outbound calls receive appropriate attestation levels in compliance with FCC requirements.

2.2 Caller-ID Control

By default, TECHNOLOGY CABLING assigns Direct Inward Dialing (DID) numbers to customers and does not permit user-supplied caller-ID information. Exceptions are made only under a written agreement that specifies the exact caller-ID values the customer is authorized to use. Such values are validated prior to being allowed on the network. If a call presents a caller-ID that does not match the authorized values on file, the call is rejected, and the customer is promptly notified to resolve the discrepancy.

2.3 Rate Limiting

Standard residential accounts are limited to a maximum of two concurrent calls. Commercial or bulk-use accounts may exceed this limit only under a formal agreement that defines permitted concurrency based on the number of active DIDs and expected conversational usage patterns. Any sudden, sustained saturation of outbound capacity triggers an automatic suspension of outbound dialing privileges until TECHNOLOGY

CABLING can contact the customer to confirm that their systems have not been compromised and that their usage remains within agreed parameters.

2.4 Call Detail Record (CDR) Monitoring

TECHNOLOGY CABLING conducts weekly reviews of CDRs for all customers, analyzing metrics including call attempt volume, Answer-Seizure Ratio (ASR), Average Call Duration (ACD), call duration distribution, and the proportion of calls shorter than 60 seconds. These metrics are compared against each customer's stated operational profile (from KYC records) and typical residential usage patterns.

Customers exhibiting signs of automated dialing, significant deviations from historical behavior, or unusually high rates of unanswered calls are contacted immediately for an explanation. If no satisfactory response is received within 72 hours, the account is suspended.

Additionally, TECHNOLOGY CABLING aggregates CDR data across accounts to identify potential sim-boxing or account aggregation schemes. Where multiple accounts originate from the same IP address or location and display patterns indicative of robocalling, we contact the responsible parties and suspend all affected accounts if a valid explanation is not provided.

3. Policy Safeguards

TECHNOLOGY CABLING enforces strict operational policies aligned with FCC mandates and industry best practices to deter robocall abuse and ensure rapid remediation.

3.1 Contractual Prohibitions

All customers are contractually bound to refrain from using the service for high-volume outbound calling, dialer-system integration, telemarketing, or the origination of any robocall—whether legal or illegal. Violation of these terms results in immediate account termination.

3.2 Know Your Customer (KYC) Requirements

Prior to service activation, every customer must provide a verifiable physical address, full legal name, email address, and an existing phone number. Business customers must also supply a valid business registration number and use an email domain associated with their registered entity. TECHNOLOGY CABLING accepts payments exclusively via credit card or bank transfer to ensure traceability.

3.3 Know Your Upstream Provider (KYUP)

TECHNOLOGY CABLING only accepts traffic from upstream providers that are regulated

carriers and listed in the FCC's Robocall Mitigation Database. Should any upstream provider be removed from that database, TECHNOLOGY CABLING will immediately cease accepting traffic from them. Prior to entering into new carrier agreements, we conduct due diligence to confirm the legitimacy of the prospective partner and verify that they maintain adequate anti-abuse protections.

4. Traceback Cooperation

TECHNOLOGY CABLING is committed to responding to all traceback requests within 24 hours of receipt. Upon receiving a traceback, we conduct a detailed review of the identified customer's CDRs for the preceding 30 days. We then engage the customer to explain any anomalies, including the specific traceback incident. If a satisfactory explanation is not provided within 72 hours, the customer's account is suspended. Any customer that is the subject of three traceback requests within a rolling 90-day period is permanently banned from our platform, unless the traceback instances are conclusively demonstrated to be lawful and compliant.
