

TELTECH ADVANCED PHONE SYSTEMS CORP
1043 53rd St, 3R
Brooklyn, NY 11219
+1 718-957-7771

Robocall Mitigation Plan

Overview

TELTECH ADVANCED PHONE SYSTEMS CORP (TELTECH) is responding to the FCC Enforcement Bureau Order EB-TCD-24-00036891 Adopted and Released on December 10, 2024 whereby TELTECH is listed as having a deficient Robocall Mitigation Database listing.

TELTECH advises the FCC Enforcement Bureau that it has initiated the process to become fully Stir/Shaken compliant but this process has only been partially implemented. Within the next 30 to 60 days, we expect Stir/Shaken to be fully implemented. TELTECH has applied to NECA for an OCN registration and will apply with iconectiv for STI-PA registration shortly afterwards. Once the STI-PA registration process is complete, TELTECH will contract with a Certified Authority to complete the Stir/Shaken setup process. TELTECH expects to be fully compliant at that time. TELTECH 's Stir/Shaken registration is should be complete during January or February 2025.

TELTECH has not been prohibited from filing a certification in the Robocall Mitigation Database.

TELTECH does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations.

TELTECH uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls.

Know Your Customer

We follow the caller ID authentication best practices for vetting caller identity and operational legitimacy for new and existing customers as described by the NANC Call Authentication Trust Anchor Working Group.

This process includes the collection and review of entity-identifying information to confirm that we have an authenticated relationship with the customer. We use this authenticated information to determine whether the customer is subject to any enforcement actions that restrict the type of calling that they may do, for example, if they have been banned from initiating telemarketing calls.

Traceback

We respond within 24 hours to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. We cooperate fully with such entities in investigating and stopping any illegal robocallers that use our service to originate, carry, or process illegal robocalls.

Robocall Mitigation Program

We will use call analytic software to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls when our implementation is complete.

The software provides detailed reporting to identify suspected illegal robocalls. The system alerts us if any outbound calls are processed where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list.

We immediately investigate any identified suspicious calls to determine if the caller attempted to originate or transit unlawful robocalls. If we determine that the traffic was likely unlawful, then we warn them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then we terminate their service.

In the Commission's release, In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 17-97 (rel. March 17, 2023) ("R&O") it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outlines "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that an RMP include:

- "know your customer" procedures;
- "know your upstream provider";
- ownership information;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Purpose

TELTECH is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. As certified in the FCC's Robocall Mitigation Database, TELTECH has fully implemented STIR/SHAKEN. In compliance with the R&O, TELTECH submits this RMP and certification.

Know Your Customer ("KYC")

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with TELTECH in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

New subscribers go through identity verification protocols which are a mixture of algorithmic check and manual call back. A risk score is developed to ensure the authenticity of a new subscriber. This score checks the identity marker collected during an account registration process. These include but are not limited to: name, email address, credit card information and contact phone number. These identity markers are validated for accuracy against public and paid tools. All new subscriber activity is monitored and limited by a Usage Policy designed for new customers. Existing customers are moved to a less limiting Usage Policy as we develop trust that the account is not compromised and is being used for its intended purpose and have a better understanding of their regular usage needs. Usage Policies are always limiting and users that intend to increase usage beyond their policy limits must submit a request to be assigned a new Usage Policy and provide justification.

Acceptable Use Policy ("AUP")

TELTECH maintains an AUP that subscribers must agree to before being permitted to use TELTECH 's system.

Know Your Upstream Provider

TELTECH 's agreements with its upstream providers contain no provision specific to robocall mitigation. TELTECH has, however, received assurances from those providers that they will sign calls transmitted to TELTECH , and will work closely with TELTECH to mitigate illegal robocall traffic. TELTECH confirms that the upstream providers have a registration in the Robocall Mitigation Database. The company will not accept voice traffic from an unregistered provider.

Monitor Traffic With Analytics

TELTECH works with its upstream carrier to analyze high-volume voice traffic in order to identify and monitor patterns consistent with robocalls. If TELTECH detects a calling pattern consistent with illegal robocalls, we will identify the party and will take appropriate action. Taking appropriate action may include, but is not limited to, initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party's ability to originate calls on our system. No third-party vendors are involved in deploying TELTECH 's analytics.

Investigate Suspicious Activity

TELTECH investigates suspicious activity found by its monitoring systems or reported to TELTECH by subscribers or third parties. The investigation could potentially result in opening a traceback request or with TELTECH contacting a subscriber to correct improper use of the platform, or, if the subscriber does not respond or comply, to block their use of the platform. TELTECH is familiar with and uses best efforts to follow the Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, TELTECH will devote sufficient resources to provide prompt and complete resources to traceback requests.

Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. TELTECH will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue. In the event of any material change to this plan, TELTECH will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Contact Information

Naftuly Wiesel, President
+1 718-957-7771
naftuly@teltech.info