

Houston TechSys LLC Robo Calling Mitigation Plan

UPDATED - FEBRUARY 2026

Houston TechSys LLC, based in Cypress, Texas, operates as a Managed Service Provider (MSP) that originates voice traffic to the public switched telephone network (PSTN). We support clients using a 3CX Voice Server solution with Telnyx trunks, and Telnyx digitally signs all our outbound trunk traffic using Houston TechSys LLC's STI certificate issued by an approved STI Certificate Authority. Additionally, we maintain a robocall mitigation program consistent with 47 CFR § 64.6305, including STIR/SHAKEN caller ID authentication implemented pursuant to 47 CFR § 64.6301(a).

Policy Overview

The following policies are in place to mitigate Robo Calling traffic that may originate from our services:

- **Customer onboarding and vetting (KYC):** At onboarding, we collect and verify the customer's legal company name, primary contact information, business address, and federal EIN. We validate potential customers by reviewing submitted information for accuracy and consistency, confirming business legitimacy through standard verification methods, and ensuring the requested services align with our offerings. We also gather expected use case and anticipated service volume to assess risk and operational fit. Enhanced review is triggered for incomplete or inconsistent information, elevated usage patterns, high risk industries, or requests that fall outside normal service profiles.
- **Caller ID integrity and attestation:** All outbound calls must include accurate caller information and a valid calling telephone number. Houston TechSys LLC assigns attestation levels based on verification of the calling party and confirmation of the party's authority to use the associated telephone number(s), consistent with applicable FCC rules, orders, and guidance. Telnyx, as the underlying DID provider and STIR/SHAKEN signing provider, performs the technical signing and transmits the applicable attestation information for outbound calls in accordance with STIR/SHAKEN protocols.
- **Monitoring and response:** We use platform level traffic analytics and monitoring tools to identify anomalous calling patterns indicative of fraud or abuse, including abnormal call volumes, burst traffic, low ASR, short duration calls, invalid or spoofed caller ID patterns, and unusual geographic routing behavior. These analytics are continuously reviewed through built-in carrier and platform monitoring systems, and where applicable, supported by upstream service provider fraud detection controls. When suspicious or

illegal traffic is detected, we follow a graduated enforcement process that may include customer notification, traffic blocking or rate limiting, temporary suspension, and escalation to full service termination if the issue is not promptly remediated. Immediate blocking or termination may occur in cases of confirmed fraud, regulatory risk, or network integrity threats.

- Prohibited use cases: Customers are restricted from initiating automated outbound campaigns. Customers are prohibited from using auto-dialers.

Compliance and Cooperation

We fully pledge our commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium. We are dedicated to fully cooperating with such entities in investigating and halting any illegal robocallers that use our services. In addition, Houston TechSys LLC reviews and maintains its robocall mitigation program and updates it within 10 business days when filing information, services, traffic patterns, or risk controls change.

Policy Enforcements

As a matter of strict company policy, we do not allow call centers or digital-only providers (voice or SMS) to utilize our services. To date, we have received no complaints of 'robocall' type services nor have we been approached by any law enforcement agency or otherwise for any assistance regarding our voice traffic.

Logging and Tracking

All our servers maintain strict and diligent logs of outbound traffic. This traffic is also tracked and digitally signed in accordance with the STIR/SHAKEN guidelines mandated by the FCC and facilitated by Telnyx.

This document outlines Houston TechSys LLC's commitment to preventing and mitigating the impact of unauthorized and illegal robocalling activities, ensuring compliance with all relevant regulatory frameworks, and maintaining the integrity of our communication services.