



Telnyx Robocall Mitigation Plan

V4.0

1 Robocall Mitigation Plan

Recent Author:	Olive Morris
Title:	Regulatory and Government Affairs Associate
Contact:	Olive Morris, regulatory@telnyx.com & olive@telnyx.com
Policy Type:	Compliance
Version:	4.0
Last Update:	February 26, 2026
Next Review:	1-year or until superseded

2 Document Control

2.1 Document Title: Robocall Mitigation Plan

2.2 Version History

1.0	5/14/2021	Fernando de Moura and Sarah Halko	Initial Version
2.0	1/26/2024	Olive Morris	Revised Version
3.0	1/10/2025	Olive Morris	Revised Version
4.0	1/08/2026	Olive Morris	Revised Version

2.3 Approvals

David Casem	CEO	5/14/2021	1.0
David Casem	CEO	02/26/2024	2.0
David Casem	CEO	01/11/2025	3.0
David Casem	CEO	02/26/2026	4.0

3 Overview

Telnyx LLC (“Telnyx” or “We”) is an interconnected voice over internet protocol (“VoIP”) provider with direct access to numbering resources pursuant to a license from the Federal Communication Commission (“FCC” or “Commission”). Telnyx delivers voice, messaging, and other telecommunications and telecommunications-related services via a web-based platform and API to power global applications and next-generation communications. Telnyx primarily services large enterprises who wish to drive further automation and control over their business communications.

As an interconnected VoIP provider, Telnyx has closely followed the FCC’s implementation of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act. Such implementation includes the required employment of STIR/SHAKEN caller ID authentication technology in the Internet Protocol (IP) portions of its network.

Telnyx has certified in the Robocall Mitigation Database that it has fully implemented STIR/SHAKEN and has instituted a Robocall Mitigation program to prevent Telnyx from originating illegal robocalls. Telnyx also certifies that any prior certification has not been removed by Commission action and Telnyx has not been prohibited from filing in the Robocall Mitigation Database.

4 SHAKEN/STIR Compliance

Telnyx has fully implemented STIR/SHAKEN into our IP network. We are compliant with all relevant FCC Orders pertaining to caller ID authentication technology requirements and STI-GA policy mandates. Additionally, Telnyx actively participates in industry discussions on robocall mitigation, including through the IP-NNI Task Force, the SIP Forum, VON, Industry Traceback Group (ITG), and other forums to remain up to date on pending and accepted best practices and ensure compliance with FCC mandates.

5 Telephone Number Authorization

Telnyx’s Telephone Number (TN) authorization is primarily based on Telnyx’s direct assignment of a TN to our customer either via purchase on our portal or API, or successful port onto the Telnyx network. When originating a call, Telnyx checks the calling party number and provides appropriate attestation to the call based on industry standards and best practices.

6 Acceptable Use Policy

All new subscribers are contractually obligated to abide by our Acceptable Use Policy (AUP)¹ and Terms and Conditions of Service² prior to accessing and using services.

Telnyx’s AUP clearly stipulates that our services cannot be used for illegal, improper, and/or inappropriate purposes. Illegal purposes include but are not limited to using any service in connection with the violation of or to violate any laws or engaging in threatening, abusive, harassing, defamatory, libelous, malicious, deceptive, or fraudulent behavior.

Among other improper and/or inappropriate uses, Telnyx’s AUP includes sending unsolicited calls and messages (including, without limitation, commercial advertising and informational announcements) if the aforementioned unsolicited activities could reasonably be expected to or do, in fact, provoke complaints.

¹ <https://telnyx.com/acceptable-use-policy>

² <https://telnyx.com/terms-and-conditions-of-service>

Telnyx's Terms and Conditions of Service state that if Telnyx receives a request from a traceback administrator authorized by the ITG for information about suspicious robocalls that have been sent to a downstream provider, the customer will promptly respond to the traceback request in good faith. Also, Telnyx may terminate the agreement, any service, or both immediately if the customer fails to comply with Telnyx policies.

7 Telnyx Customer KYC, Monitoring, and Fraud Prevention

Telnyx takes the following steps to minimize the risk of fraud originating on our network:

Every new account goes through Telnyx's proprietary fraud screening process at sign up. As part of that process, customers must complete mandatory phone number verification to prevent a single individual from creating multiple accounts. Customers progress through a tiered account verification system: starting from trial level, which places extensive restrictions on customers' outbound dialing capabilities, and progressing to higher tiers, which require more robust Know Your Customer (KYC) identity verification, including document review, business validation, and measures designed to evaluate and assess the customer's business legitimacy, use case, and overall risk profile. Telnyx actively monitors traffic patterns, including answer success rates (ASR) and average call duration (ACD), across all new and existing customers and immediately takes steps to block accounts if these patterns reflect fraudulent activity. In addition, Telnyx has implemented third-party analytics providers (e.g., RRAPTOR and Nomorobo) that monitor traffic patterns to alert our fraud team of suspicious activity or calling patterns.

Telnyx blocks originating calls with invalid ANI and maintains a Do Not Originate list to catch potential fraudulent calls before they leave our platform. In addition to calling patterns, Telnyx has implemented payment method tracking to block customers with suspicious payment activities.

8 Investigation of Suspicious Activity and Traceback

Telnyx communicates with customers to share the latest FCC orders and industry best practices for complying with robocall mitigation technologies and minimizing fraud origination on our collective networks. As such, we have encouraged our customers to participate in the ITG and require cooperation with the ITG in our Terms and Conditions of Service. Telnyx endeavors to respond to Commission and ITG traceback requests within 24 hours.

Any alert sent to Telnyx via our internal monitoring, tracebacks, and vendor alerts are reviewed by our fraud team, and a determination is promptly made on whether to remove the customer from our platform.

9 Blocking

Telnyx offers Inbound Call Screening to our customers, enabling users to flag and block unwanted incoming calls to maintain the integrity of their communications. Our Inbound Call Screening employs the STIR/SHAKEN attestation protocol to validate the authenticity of Caller ID information and includes two features: Enhanced Call Control and Spam Call Detection. With Enhanced Call Control, users can reject or flag suspicious calls based on customizable conditions. With Spam Call Detection, users can effectively identify and screen potential spam calls to protect Telnyx numbers from unwanted solicitations and fraudulent activities.

10 Plan Updates

Telnyx's continued participation in various industry working groups allows us to monitor updates to best practices and continuously improve our internal processes to ensure our practices continue to evolve to meet new threats.