

Robocall Mitigation Program

1. Introduction This Robocall Mitigation Program outlines the policies and practices implemented by DML IT Solutions to prevent the transmission of illegal robocalls through our network. This program ensures compliance with the Federal Communications Commission (FCC) rules and the requirements of the Robocall Mitigation Database (RMD).

2. Scope This program applies to all traffic transmitted through DML IT Solutions network in its role as a non-gateway intermediate provider.

3. Designation

- Non-Gateway Intermediate Provider

4. Robocall Mitigation Practices

4.1. Call Authentication and STIR/SHAKEN Implementation Pursuant to the Second Report and Order, Paragraph 19, DML IT SOLUTIONS is a non-gateway intermediary provider that “voice service providers which lack control over the network infrastructure necessary to implement STIR/SHAKEN are not subject to our implementation requirements.”

Voice service providers, gateway providers, and those non-gateway intermediate providers that receive unauthenticated Session Initiation Protocol (SIP) calls directly from an originating provider are required to implement STIR/SHAKEN. See 47 CFR §§ 64.6301(a), 64.6302(c), (d). Non-gateway intermediate providers that do not receive unauthenticated SIP calls directly from originating providers and providers who lack control over the network infrastructure necessary to implement STIR/SHAKEN do not have an implementation obligation.

As a result, we do not receive unsigned calls from sip carriers and merely transmit data between upstream carriers like Telnyx LLC, which control and handle the signing and mitigation of calls for STIR / SHAKEN compliance. The following section 4.2 shows an attestation from our upstream carrier showing their robocall mitigation practices.

4.2 Attestation by Telnyx, LLC

3 Overview

Telnyx LLC (“Telnyx” or “We”) is an interconnected voice over internet protocol (“VoIP”) provider with direct access to numbering resources pursuant to 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 their networks.

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

4 SHAKEN/STIR Compliance

Telnyx has fully implemented SHAKEN/STIR 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 at IPNNI, the SIP Forum, VON, 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 against Telnyx’s inventory and will provide appropriate attestation to the call based on industry standards and best practices.

Nonetheless, if a Telnyx customer wishes to use a TN as a caller identity and that Telnyx does not directly manage TN, then attestation adjustments can be made if the Telnyx customer meets the following conditions: they are an existing Telnyx customer, they can provide proof of a know your customer or TN validation process for their customers, and they have received no industry complaints (tracebacks, vendors, or subpoenas) in their tenure with Telnyx.

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

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

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

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 aforementioned unsolicited activities could reasonably be expected to or do, in fact, provoke complaints.

Telnyx's Terms and Conditions state that if Telnyx receives a request from a traceback administrator authorized by the Industry Traceback Group 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 company policy upon becoming a Telnyx user.

7 Telnyx Customers, Monitoring, and Fraud Prevention

Telnyx collects contact and company information for each new customer upon sign-up. In line with our AUP and Terms and Conditions, Telnyx can leverage such contact information when we detect fraudulent call patterns to notify the customer of potential blocking or to pass such contact information to traceback administrators or law enforcement agents when necessary.

Telnyx takes the following steps to minimize the risk of fraud originating on our network. First, Telnyx blocks any subscribers who attempt to sign up with a "free-mail" account to reduce the risk of inviting bad actors onto our platform. Upon signing up with a valid e-mail, Telnyx customers are significantly limited to the amount of traffic they can originate from our platform. Suppose the customer wishes to increase their origination thresholds. In that case, they can apply for "level 2 verification," which includes a more in-depth review of the company's calling patterns, business model, and any previous complaints. Telnyx monitors traffic patterns, primarily tracking answer success rates ("ASR") and average call duration ("ACD"), by all new and existing customers and immediately takes steps to block the account if the patterns mentioned above reflect fraudulent activity. In addition to internal monitoring tools, we have implemented a third-party analytics provider (Nomorobo) that monitors traffic patterns through machine learning to alert our fraud team of suspicious activity or calling patterns. Telnyx currently blocks any originating call with an invalid ANI and is in the process of implementing the US Telecom DNO list to ensure we catch any potential fraudulent call from leaving our platform. In addition to calling patterns, Telnyx has implemented payment method tracking to block any customer with suspicious payment activities.

8 Investigation of Suspicious Activity and Traceback

Telnyx always communicates with new and existing 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 all our customers to participate in US Telecom's Traceback group and have included these requirements in our services' Terms and Conditions. Telnyx actively participates in Traceback requests and ensures to respond within 24 hours to all such requests from the Commission, law enforcement, and the industry traceback consortium.

Any alert sent to Telnyx via our internal monitoring, tracebacks, and vendor alerts are properly reviewed by our fraud team, and a determination is made 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 SHAKEN/STIR 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 our Spam Call Detection feature, users can effectively screen and identify potential spam calls to protect Telnyx numbers from unwanted solicitations and fraudulent activities, and avoid spam calls. As SHAKEN/STIR and other industry robocall mitigation efforts are implemented, we will be sure to monitor conditions for blocking fraudulent calls from reaching our customers.

10 Plan Updates

Telnyx's continued participation in various industry working groups will allow us to monitor updates to best practices and continuously improve our internal processes to ensure our Robocall Mitigation Plan continues to evolve with these threats.

5. Reporting and Certification DML IT Solutions has filed its certification with the FCC's Robocall Mitigation Database, attesting to compliance with the applicable requirements for non-gateway intermediate providers. This certification includes:

- Contact details for a responsible officer.
- A detailed description of implemented mitigation practices.

6. Enforcement and Accountability We enforce this program through internal compliance checks and audits. Any upstream or downstream provider found to be non-compliant is subject to traffic blocking or termination of business relationships.

7. Collaboration with Industry and Regulators DML IT Solutions participates in industry forums and collaborates with regulators to:

- Share information about robocall mitigation best practices.
- Address emerging threats in illegal robocall traffic.
- Improve call authentication standards across networks.

8. Updates and Maintenance This program will be reviewed annually or as needed to reflect changes in FCC regulations, industry standards, or new technological developments.

9. Contact Information For inquiries related to this program, please contact:

Brandon Jarosch
IT Manager
714-966-0345
brandon@dmlitsolutions.com

Acknowledgment This document reflects DML IT Solutions commitment to mitigating illegal robocalls and maintaining the integrity of our network as a non-gateway intermediate provider.